AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE	OF	PAGES
U	1		2

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUISITION NUMBER	5. PROJECT NUMBER *(If applicable)*
P00001	10/04/2022	1300889192	N/A

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE	SCD
NAVWAR-NIWC Atlantic (CHRL) P.O. BOX 190022 North Charleston, SC 29419-9022	N65236	DCMA MUNITIONS AND SUPPORT SYSTEMS SPRINGFIELD BLDG. 1, ARDEC PICATINNY, NJ 07806-5000	S3101A	C

8. NAME AND ADDRESS OF CONTRACTOR *(Number, street, county, State and ZIP Code)*

Engineering Services Network
13580 Groupe Drive, Suite 402
Woodbridge, Virginia 22192-4166

CODE 05BD7 FACILITY CODE 933578825

(X) ☐ 9A. AMENDMENT OF SOLICITATION NUMBER

9B. DATED *(SEE ITEM 11)*

☒ 10A. MODIFICATION OF CONTRACT/ORDER NUMBER
N0017819D7599/N6523622F3047

10B. DATED *(SEE ITEM 13)*
09/29/2022

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to he hour and date specified in the solicitation or as amended, by one of the following me hods: (a) By completing items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA *(If required)*

SEE SECTION G

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.

CHECK ONE	
☐	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: *(Specify authority)* THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
☐	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES *(such as changes in paying office, appropriation data, etc.)* SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
☐	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
☒	D. OTHER *(Specify type of modification and authority)* Mutual Agreement of the Parties, FAR 43.103(a)(3)

E. IMPORTANT: Contractor ☐ is not ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (*Organized by UCF section headings, including solicitation/contract subject matter where feasible)*

SEE PAGE 2

Except as provided herein, all terms and conditions of he document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER *(Type or print)*		16A. NAME AND TITLE OF CONTRACTING OFFICER *(Type or print)*	
(b) (4), (b) (6)		Christie Hazlett , Contracting Officer	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(b) (4), (b) (6) *(Signature of person authorized to sign)*	10/04/2022	/s/Christie Hazlett *(Signature of Contracting Officer)*	10/04/2022

General Information

1) Section B: (b) (4)
2) Section C: Revised Section 13.1 Authorized Subcontractors and included the subcontractors, which were evaluated during negotiations.
3) (b) (4)
.

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 91

1. CONTRACT/PURCH ORDER/AGREEMENT NO.	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMMDD)	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
N0017819D7599	N6523622F3047	2022OCT04	1300889192	Unrated

6. ISSUED BY CODE N65236

NAVWAR-NIWC Atlantic (CHRL)
P.O. BOX 190022
North Charleston, SC 29419-9022

7. ADMINISTERED BY *(If other than 6)* CODE S3101A

DCMA MUNITIONS AND SUPPORT SYSTEMS SPRINGFIELD
SCD: C
BLDG. 1, ARDEC
PICATINNY, NJ 07806-5000

8. DELIVERY FOB
- ☐ DESTINATION
- ☐ OTHER *(See Schedule if other)*

9. CONTRACTOR CODE 05BD7 FACILITY 933578825

NAME AND ADDRESS
Engineering Services Network
13580 Groupe Drive, Suite 402
Woodbridge, VA 22192-4166

10. DELIVER TO FOB POINT BY *(Date) (YYYYMMMDD)*
SEE SCHEDULE

11. X IF BUSINESS IS
- ☒ SMALL
- ☐ SMALL DISAD-VANTAGED
- ☐ WOMEN-OWNED

12. DISCOUNT TERMS
Net 30 Days WAWF

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
SEE SECTION G

14. SHIP TO CODE
SEE SECTION F

15. PAYMENT WILL BE MADE BY CODE HQ0337
DFAS Columbus Center, North Entitlement Operations
P.O. Box 182266
Columbus, OH 43218-2266

MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.

16. TYPE OF ORDER
- DELIVERY/CALL ☒ This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.
- PURCHASE ☐ Reference your ____ furnish the following on terms specified herein.

ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.

NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMMDD)
Engineering Services Network		(b) (4), (b) (6)	

☐ If this box is marked, supplier must sign Acceptance and return the following number of copies:

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE
SEE SCHEDULE

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	SEE SCHEDULE				

*If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.

24. UNITED STATES OF AMERICA
BY: /s/Christie Hazlett 10/04/2022
CONTRACTING/ORDERING OFFICER

25. TOTAL (b) (4)
26. DIFFERENCES

27a. QUANTITY IN COLUMN 20 HAS BEEN
☐ INSPECTED ☐ RECEIVED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	c. DATE (YYYYMMMDD)	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	28. SHIP. NO.	29. D.O. VOUCHER NO.	30. INITIALS
	☐ PARTIAL ☐ FINAL	32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR
f. TELEPHONE NUMBER / g. E-MAIL ADDRESS	31. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL		34. CHECK NUMBER
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT. a. DATE (YYYYMMMDD) / b. SIGNATURE AND TITLE OF CERTIFYING OFFICER			35. BILL OF LADING NO.

37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED (YYYYMMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

Section C - Description/Specifications/Statement of Work

SECTION C – DESCRIPTION/SPECS/WORK STATEMENT

SPECIFICATIONS/STATEMENT OF WORK/PERFORMANCE WORK STATEMENT

Work under this performance-based task order will be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein will be referred to as Performance Work Statement (PWS):

SHORT TITLE: BUSINESS APPLICATIONS IN SERVICE ENGINEERING AGENT (BA ISEA) INTEGRATED PRODUCT TEAM (IPT) TECHNICAL SUPPORT

1.0 PURPOSE

1.1 SCOPE

This PWS covers program management, modernization, logistics engineering, sustainment engineering and hardware engineering, independent verification and validation, and training support services for Naval Information Warfare Center (NIWC) Atlantic in support to the Program Executive Office for Manpower, Logistics and Business Solutions (PEO MLB), Logistics (LOG) Information Technology (IT) Services Delivery Team. This support encompasses sustaining Maintenance Figure of Merit (MFOM) Family of Systems (FoS) (thereinafter referred as the MFOM system) and Naval Tactical Command Support System (NTCSS) current solutions as well as transitioning and integrating the MFOM and NTCSS existing capabilities into PEO MLB LOG IT Services Delivery Team's future Naval Operational Business Logistics Enterprise (NOBLE) FoS.

NOTE: Website and e-mail addresses referenced within the PWS and Contract Data Requirements List (CDRL) forms are subject to change. For any website and e-mail address not working during time of performance, the contractor shall contact the Contracting Officer's Representative (COR) or Contracting Officer for latest website and e-mail address. An incorrect website or e-mail address does not alleviate a contractor from required reporting or access requirements.

1.1.1 Multiple Funding

This task order is funded with multiple appropriations as delineated on specified contract line item numbers (CLINs). The applicable PWS task(s) associated with each CLIN is outlined in Section B and Section G.

1.2 BACKGROUND

BA ISEA IPT encompasses ISEA functions across legacy programs including MFOM, NTCSS, and anticipated future FoS programs. In this way, the IPT seeks to leverage the same human resources across multiple programs in order to gain efficiencies and economies of scale.

BA ISEA's responsibility is to deploy the software to the field/end-user and ensure the software is working. BA ISEA's focus is to provide hardware upgrades and replacements, deploy/install updated software to the end-user, and provide Service Desk support to the end-users to assist with resolving issues. The BA ISEA does not make changes to the software. If software changes are required, the software is assessed and software changes are executed by software developers which are not part of the BA ISEA IPT.

MFOM system is a web-based family of software applications that operate on classified and unclassified networks both ashore and afloat, calculating a unit's material readiness, and displaying maintenance and readiness information in various formats that support the chain of command from the Office of the Chief of Naval Operations (OPNAV) to the Sailor. MFOM provides near real-time material-based readiness reporting to the Defense Readiness Reporting System-Navy (DRRS-N), improves the Naval maintenance community's IT, improves the accuracy of the material-based readiness values, and improves the Naval maintenance community's worker and workload efficiencies. MFOM is a diverse maintenance, logistics and readiness reporting software solution with multiple components including a computing infrastructure, a cross domain solution, a multitude of configuration items, backend databases, ship/shore equipment models, communication, and messaging suites, and 16 user facing software applications that operate on classified and unclassified networks both ashore and afloat. The BA ISEA IPT does not make changes to the MFOM software, the BA ISEA deploys the software Afloat to the end-user/ships after it's changed or modified and tested.

NTCSS is a logistics command and control support information system for management of ships, submarines, aviation squadrons, and intermediate maintenance activities (afloat and ashore) and is designated as a Mission Essential, Acquisition Category (ACAT) in accordance with, Major Automated Information System (MAIS). NTCSS is an open architecture client-server system using a common server and

operating environment with tactical systems and provides a full range of application segments to satisfy readiness and logistics business needs of the Navy. NTCSS is a roll-up of several independent legacy systems including the Shipboard Non-Tactical Automated Data Processing (ADP) Program and Naval Aviation Logistics Command Information System. It is the support side of the Joint Maritime Command Information System, with NTCSS Afloat as the tactical side. The BA ISEA IPT does not make changes to the NTCSS software, the BA ISEA deploys the software Ashore and Afloat to the end-user after it's changed or modified and tested.

The PEO MLB LOG IT Services Delivery Team, the assigned Navy Program Office to manage MFOM and NTCSS, is executing future program strategies to replace and integrate the MFOM and NTCSS capabilities into their future FoS Program. The future FoS program is currently referred to as NOBLE, including Naval Operational Supply System (NOSS) and Naval-Maintenance, Repair and Overhaul (N-MRO). However, it is expected that plans will change and this program will continue to morph as the program office seeks to overcome affordability challenges. The BA ISEA IPT is expected to support whatever product eventually materializes. This includes internal IPT processes as well as Naval Information Warfare Systems Command (NAVWAR) enterprise procedures, processes, and policy. It is anticipated that this IPT's software may be utilized as proof of concept or our team may be requested to assist in rewriting new enterprise processes.

2.0 PLACE(S) OF PERFORMANCE

2.1 GOVERNMENT FACILITIES

Government facilities (i.e., office space or lab space) are provided to those contractor personnel that would otherwise adversely affect the work performance if they were not available on Government site. Labor categories with supplied Government facilities shall be located at 1837 Morris Street, Bldg. Z133, Norfolk, VA 23511 or 9456 4th Avenue, Bldg. V53, Norfolk, VA 23511.

2.1.1 Access to Government facilities

NIWC Atlantic and other Government installations have restricted access. Contractors are limited to access during certain days and times as specified in the workweek requirements of this PWS. If access to the assigned Government facility is restricted due to safety/security exercise, an Executive Order, or an administrative leave determination applying to the local activity (e.g., inclement weather), the contractor, in agreement with the COR, shall make alternative work arrangements. The contractor shall adjust work schedule, work at an alternate location, or if alternate work arrangements cannot be accommodated, the contractor shall notify the COR of the inability to access the assigned facility prior to charging their time to the task order as direct cost provided such charges are consistent with the contractor's accounting practices. The ability to work at an alternate location that is not a Government or contractor facility site is dependent on the contractor having an alternative work site agreement with the employee. The ability to work at an alternate location may not be an option for certain support services.

2.1.2 Training Requirements and Exercise Support

Contractor personnel working full-time or partially at a Government facility shall complete all applicable training requirements as specified under Mandatory Training, PWS Para 8.0. Contractor personnel may also be required to participate in safety, security (e.g., Anti-Terrorism Force Protection (AT/FP)), and operational training exercises (possibly two per year). Applicable contractor personnel shall support and participate in the training exercise which may include role-playing and reacting to exercise injects based on the situation or exercise objectives.

2.1.3 Emergency Management at Government Installations

During emergency situations including health (e.g., COVID-19 pandemic) and weather related circumstances, contractor personnel with scheduled access to a Government installation shall coordinate with the COR prior to reporting to their Government worksite. Access will be in accordance with the latest Government installation requirements and restrictions. The contractor shall identify with the COR if certain personnel are designated mission essential and determine the work expectations during the emergency period of performance. Depending on the type of support, working from an alternative worksite may or may not be allowed.

2.2 CONTRACTOR FACILITIES

A significant portion of work issued under this task order requires close liaison with the Government. The contractor shall be prepared to establish a local facility within a thirty (30)-mile radius of NIWC Atlantic Norfolk facility located at 1837 Morris Street, Bldg. Z133, Norfolk, VA 23511 and /or 9456 4th Avenue, Bldg. V53, Norfolk, VA 23511. The contractor shall be capable of quickly interfacing with the secure labs located at NIWC Atlantic. The contractor's facility is not necessarily for the exclusive use of this task order and can be utilized on a shared basis. The contractor shall meet all facility location and size requirements within 30 days after task order award. The contractor shall ensure facility includes space for offices, conference rooms, lab work, and a staging area for materials and equipment.

2.3 ALTERNATE WORK LOCATIONS

The ability to provide support from an alternate location (includes working from an employee's residence or other non-Government facility) is dependent on the type of support required, the contractor employee's ability and trustworthiness, and the company's employment policy. Allowing work to be performed at an alternate location is not an option for all positions and personnel. The ultimate decision to allow work

performed at an alternate work location will be determined by the COR. If alternate work locations are allowed, the company shall have defined criteria addressing the minimum requirement to have continuous, secure internet connectivity. Each applicable contractor employee shall have an established signed telework agreement between the company and employee. For each contractor employee proposed to work at an alternate location, the contractor shall submit a written request and justification to the COR with a copy of the applicable employee's signed telework agreement which becomes part of the COR files. If the requirements for teleworking and/or alternate work locations are not outlined/specified in the employee agreement documentation, the contractor shall include a copy of those requirements with the signed employee agreement. Working at an alternative location shall not adversely affect the response time required in support of the task order. The Government reserves the right to disallow any billable hours by contractor employees working at an alternative work location without obtaining prior Government approval. The Government reserves the right to discontinue the ability to work from an alternate location at any time without cause. The inability of a contractor to respond to the requirements of the task order due to telework conditions will be negatively reflected in the Contractor Performance Assessment Reporting System (CPARS). The contractor shall utilize the Government site or Client site (vice contractor site) overhead labor rate for personnel working from their residence unless their Accounting System requires a different billing structure.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list non-personal services tasks that will be required throughout this task order. The contractor shall provide necessary resources with knowledge and experience as cited in the personnel qualification requirement to support the listed tasks. The contractor shall perform requirements in accordance with Federal Acquisition Regulation (FAR) and/or Defense Federal Acquisition Regulation Supplement (DFARS) that do not include performance of inherently Government functions. The contractor shall complete all required tasks while controlling and tracking performance and goals in terms of costs, schedules, and resources.

The BA ISEA IPT is utilizing the Agile methodology as approved by PEO MLB LOG IT Services Delivery Team. The contractor shall meet evolving requirements while leveraging Agile best practices and robust communication between the product sponsor and the project team. Additionally, the contractor shall provide this support using the BA ISEA toolsets (e.g., JIRA/JAMA or equivalent) implemented and provided by the Government. The contractor shall support stakeholders and their respective organizations to understand, embrace, and adopt Agile methodologies, processes, and culture.

3.1 PROJECT MANAGEMENT SUPPORT (OMN, OPN)

The contractor shall provide project management (PM) services to support NIWC Atlantic in maintaining, sustaining, and enhancing the BA ISEA core applications and software components, infrastructure platforms and technologies, internal and external interfaces, as well as transitioning the current capabilities to the future FoS.

3.1.1 Program Support

3.1.1.1 The contractor shall provide program support services for planning, organizing, and managing resources to bring about the successful execution of specific program/project goals and objectives as defined in this PWS. The primary objective of this task is to achieve all of the project goals and objectives while adhering to specific project constraints (scope, quality, schedule, and cost). The contractor shall apply standards, principles, and techniques of project management to monitor, control, and direct completion of all requirements, from receipt and initiation through planning, scheduling, execution, monitoring, transition, and closure. The contractor shall document and update its progress on completing tasking in the Task Order Status Report (TOSR) (CDRL T001) that is detailed in Section 5 of this PWS. Contractor shall:

1. Plan, schedule, facilitate, and document meetings
2. Provide Subject Matter Expertise (SME) to support to the Government
3. Respond to the Government's status reporting and data call requests
4. Provide out year program and spend plan/budget planning
5. Record, track, and manage action items
6. Conduct analysis and develop Courses of Action (COAs)
7. Develop, collect, and report performance metrics
8. Provide technical writing and editing support to enhance documentation

3.1.2 Schedule Management Support

3.1.2.1 The contractor shall coordinate with the Government to develop an approach, and define the associated artifacts, to manage the schedule requirements associated with this PWS. The contractor shall tailor this plan to the overall BA ISEA execution strategy and document this approach in the Cost and Schedule Milestone Plan (CDRL T002) as outlined in Section 5 of this PWS. The contractor shall provide monthly updates to the defined schedule artifacts as part of both the TOSR (CDRL T001) and monthly Program Management Review (PMRs) (CDRL T004). The contractor shall address the following actions in the Cost and Schedule Milestone Plan (CDRL T002) as well as briefing them in the Monthly PMR (CDRL T004):

1. Manage planned events and project milestones
2. Manage task due dates and constraints
3. Manage task order deliverables
4. Manage internal and external dependencies
5. Identify and report schedule risk, issues, and variances
6. Identify recommendations and corrective actions to be implemented to mitigate risk
7. Integrate schedule data and artifacts with other Government plans and schedule artifacts

3.1.3 Cost Management Support

3.1.3.1 The contractor shall coordinate with the Government to develop an approach, and define the associated artifacts, to manage the cost associated with this task order. The contractor shall align this plan to the overall BA ISEA IPT cost and schedule strategy and document this approach and associated artifacts in the Cost and Schedule Milestone Plan (CDRL T002). The contractor shall provide a Contract Funds Status Report (CDRL T003) and discuss cost performance and results during the monthly PMRs (CDRL T004).

3.1.4 Risk Management Support

The contractor shall provide support by utilizing the risk parameters identified in the BA ISEA IPT Project Management Plan and assist in identifying and documenting all relevant risks to include mitigation strategies and contingency plans for risks, when required. The contractor shall report the total risks (including mitigation and contingency), exposure trends, and risk composite summaries to the Government during the monthly PMRs (CDRL T004).

3.1.5 Scrum Master Support

The contractor shall provide support responsible for promoting and supporting Scrum and ensuring the scrum framework is followed. The contractor shall assist the team with understanding and applying Scrum theory, practices, rules, and values. The contractor shall serve as the Scrum Master and be committed to removing impediments and helping the team become self-organizing and empowered to create, innovate, and make decisions for themselves as one team. The contractor shall lead and participate in Program Increment Planning, Scrum meetings, Sprint planning, Sprint reviews, and Sprint retrospectives.

3.1.6 Project Management Reviews (PMR)

The contractor shall coordinate, prepare, and conduct monthly PMRs (CDRL T004). The purpose of the PMRs is to ensure both the contractor and the Government have a mutual understanding of the progress and status of tasking with this PWS.

3.2 MODERNIZATION SUPPORT (OPN, OMN, RDT&E, SCN)

The contractor shall provide modernization support services for installation planning, database conversion, and system installation and turnover in CONUS, OCONUS, or aboard a ship locations. This support encompasses sustaining the BA ISEA IPT's current solutions as well as transitioning and integrating BA ISEA IPT's existing capabilities into the PEO MLB LOG IT Services Delivery Team's future FoS.

The contractor shall plan for timely delivery and installation of software and hardware such as laptop servers and application peripherals such as docking stations and printers to afloat platforms and shore sites. Providing this support in an effective and efficient manner will ensure maximum access to and implementation of ISEA technology, services, and resources.

With Agile transition in mind, the contractor support shall meet evolving requirements, metrics collection and reporting, and process/procedural changes.

Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended workweek (EWW) may be required for professional (i.e., salaried) employees.

3.2.1 Installation Planning (OPN, OMN, or RDT&E)

The contractor shall provide advanced planning support for installation planning. The contractor shall perform installation planning activities to include build plans, schedules, and work packages to support the delivery and integration of new capability into existing and new platforms, relocation of existing capability, and the removal of capability. The contractor shall support platform modernization planning and installation planning for existing platforms, as well as transition and integration planning for newly built platforms. The contractor shall support development of installation strategies and requirements, fielding plans and schedules, cost estimates, installation approval documentation, installation work scope and tasking statements, and other installation related plans and reports.

The contractor shall support activities required to obtain installation/site approval such as those required by the Navy Modernization Process (NMP), the C5I Modernization Process (C5IMP), and the Fleet Readiness Certification Board (FRCB) processes. The contractor shall support installation planning through fielding analysis of Authorization To Operate (ATO) packages, engineering documentation, Systems Administration Guides (SAG), Fielding Plans, Ship Change Documents (SCDs) and Software Delivery Documents (SWD), Plan of Action and Milestones (POA&Ms), Installation Requirements Drawings (IRDs), processes to field to environments including DevOps, systems and patches under development, ISEA hardware specifications, hardware Pre-Installation Test and Checkout (PITCO), Systems Integration Test (SIT) and Final Acceptance Test (FAT), and Electromagnetic Environmental Effects (E3) studies.

The contractor shall provide support for Installation Planning Artifacts (CDRL T005) to develop Systems Integration and Enterprise Application Request for Change (RFC) packages, System-level and Platform-level Systems Operation Verification Test (SOVTs) documents, network Boundary Change Requests (BCRs), Ship Installation Readiness and Site Survey Reports, In-Briefs, Regional Maintenance & Modernization Coordination Office (RMMCO) books for new construction ships, and contact emails for On-Site Install Coordinators or sites for pre-upgrade tasks.

The contractor shall compile and report Advanced Planning Group (APG) metrics, dashboard reports, Agile Sprint tracking and manage Sprint and datacenter meetings as directed. The contractor shall distribute Integrated Logistics Support (ILS) (CDRL T019) packages and MFOM software as directed, upload install completion deliverables to Share-point, follow up with On-Site Installation Coordinator (OSICs) for cyber-green install completion, request ship tag-out databases for conversion, order the E52/INIT files (contains all of the Automated Sequence Indicators (ASIs) at the time of creation for a specific ship) for ships maintenance system conversions to Automated Work Notification (AWN) and submit Install Design Plan (IDP) drawing inputs (CDRL T005).

3.2.2 Database Conversion Support (OMN, SCN)

The contractor shall provide database support services to build the suite of databases for shore and afloat activities and perform quality assurance (QA) activities in accordance with the BA ISEA processes and procedures. The contractor shall provide a Database Build POA&M (CDRL T006) for timely delivery of the databases to shore and afloat platforms. The contractor shall provide a QA POA&M (CDRL T006) and execute QA activities to completed suite of databases for shore and afloat activities.

3.2.3 System Installation and Turnover Support (OPN, OMN)

Programs under the BA ISEA IPT’s purview have been in the sustainment stage of the Defense acquisition lifecycle for many years. The current software installation process follows the hardware centric ship main process which is manual (boots on the ground) and resource (time and people) intensive taking approximately five years to upgrade all users. Recent innovations and advancements by software development teams have been realized resulting in software upgrade developments that are ready to deploy in approximately three weeks providing an opportunity to drastically improve Fleet operations and cyber security posture. To exacerbate the current resource intensive and time-consuming installation process, the impact of the Coronavirus Disease (COVID)-19 pandemic has underscored existing gaps and the need to close them. Specifically, PEO C4I leadership has asked product teams to use remote support, when possible, to avoid travel, minimize exposure, and maximize safety. This mandate, coupled with recent innovations and advancements by the software development teams have created an opportunity to not only drastically improve Fleet operations but also the opportunity to enable manpower, cost and schedule efficiencies to be realized throughout all impacted communities. To fully capitalize on this opportunity, current operational concepts, processes, and procedures must be adapted, improved, and/or created.

The contractor shall apply engineering, analytical, technical disciplines, and skills to establish and maintain long-term engineering, operation, and maintenance support for BA ISEA system capabilities.

The contractor shall support the execution of installation responsibilities in accordance with the BA ISEA processes and procedures. The contractor shall provide afloat and shore installation and integration plans, drawings, technical change documentation and notices, and procedures. This support includes site/platform support.

The contractor shall provide Daily Status Reports (DSR) (CDRL T007) on a daily basis for each installation it is performing until a Final DSR is submitted. The contractor shall report and include in the DSR, all defects found during installations. The DSR shall be submitted to the COR on a daily basis only when an actual installation is occurring. The DSR is not required when an installation is not occurring. The DSR shall include travel details when off-site installations are required. The DSR shall also address Training details when the installer is required to provide user training during an installation.

Except for special situations addressed in the subsection below (Exceptions to Afloat Standards) the contractor shall perform all afloat (ship and submarine) and shore installation services in accordance with the requirements contained in the current version of the NAVSEA SL720-AA-MAN-030, NAVSEA Navy Modernization Process Management and Operations Manual (NMP-MOM) also known as “One Book”, Afloat Installation Process Handbook (AIPH), and the Shore Installation Process Handbook (SIPH). All installation documentation, including Memorandums of Agreement (MOAs), Ship Installation Documents (SIDs), and SOVTs documents, delivered under this task order shall meet the technical and formatting requirements for the documents contained in the NMP-MOM and in this PWS. Installation practices shall conform to the requirements and standards identified in this PWS.

Exceptions to Afloat Standards:

The afloat (shipboard and submarine) standards shall apply to all NIWC installations even when the installation occurs on non-Navy vessels such as Military Sealift Command (MSC) Ships unless specific permission to substitute a commercial standard has been granted in writing by the BA ISEA COR. To obtain permission to substitute a commercial standard, the contractor may be required to provide a copy of the standard to the Contracting Officer, NIWC 4.2, or the cognizant Program Executive Office (PEO) Design Authority for review. In general, the Military Standards that apply to C4ISR installations can be followed on both commercial vessels and Navy ships, so permission to deviate from these standards will rarely be granted. If the installation is governed by a NIWC IRD, approval may be required from the PEO Design Authority for the IRD to allow the use of commercial standards. This internal Government process could take an indefinite period of time. The contractor shall forward any exception requests to the government Service Delivery Manager (SDM) as soon as the contractor is aware that an exception is necessary.

Mandatory Shipboard and Submarine Requirements Documents:

Adherence to the documents referenced in the Government BA ISEA processes and procedures is a requirement of this PWS during the performance of work on or for ships, submarines, and other afloat platforms. Whenever one of these standards is applicable to an installation and the standard states that something “should” be done, the contractor shall do what the standard says “should” be done unless specific permission not to do so has been granted by the COR or stated in the task order.

Shipboard and Submarine Guidance Documents:

The guidance documents referenced in the government BA ISEA processes and procedures shall be used as guidance to interpret the mandatory requirements. The contractor is permitted to deviate from the methods (how to) guidance provided in the government BA ISEA processes and procedures as long as:

1. The deviation will not increase safety risks.

2. The deviation will not cause a violation of the requirements contained in the PWS or the Mandatory Requirements Documents reference the government BA ISEA processes and procedures.

3. Alternative guidance is used that can be shown to provide an overall benefit to the Government.

The contractor shall coordinate with Regional Maintenance and Modernization Coordination Offices (RMMCO) or other Government designated gatekeepers for surface and subsurface installations/alterations.

3.2.3.1 Pre-installation Support

Ship Checks/Site Surveys - The Contractor shall conduct inspections of ships and submarines (Ship Checks) and shore sites (Site Surveys) scheduled for installs to determine the optimum location and configuration for an equipment/system installation and any site or platform preparation requirements. The Contractor shall be capable of gathering all pertinent environmental, engineering, configuration, and design information relevant to site conditions, analyzing the collected data, performing necessary calculations to make technical recommendations, and preparing Pre-installation artifacts (CDRL T008) are technical reports and documentation such as Site Survey Reports, Pre-Implementation Briefs , In-Briefs/Out-Briefs, Ship Check Reports, and DSRs (CDRL T007), for a specific installation or a group of installations.

Upon completion of a Ship Check or Site Survey, a completed Ship Check Report or Site Survey Report shall be provided to the BA ISEA IPT COR and assigned Project Lead.

3.2.3.1.1 Pre-installation Preparation Requirements

When afloat installation preparation work is required that is beyond the capacity of the contractor to perform for any reason, the contractor shall be tasked to describe in detail the work that must be performed to complete the installation.

3.2.3.1.2 Pre-installation Checkout

A Pre-Installation Check-Out (PICO) is conducted prior to commencing Modernization efforts on affected systems to identify pre-existing discrepancies which, if uncorrected, could delay or prevent successful completion of the install. PICO shall be conducted when determined by the Program Acquisition Resource Manager (PARM), ISEA, assigned Project Lead or government SDM that the complexity and risk associated with the alternation/SC warrant a PICO requirement. Thus, not all BA ISEA afloat installs will require a PICO; however, in the case that one is required, the contractor shall work with the assigned Project Lead to determine scheduling of and coordination with the ship.

3.2.3.2 Installation Support

The contractor shall provide the technical support services necessary to accomplish or support an assigned installation in accordance with a Government approved design package. Installations shall be in accordance with applicable directives and this PWS.

The contractor shall install new or upgraded software and/or hardware such as laptop servers and application peripherals such as docking stations and printers on surface ships, submarines, special purpose crafts, and shore platforms located worldwide. The contractor shall support the following tasks onboard ships and submarines and shore platforms:

1. Installation/removal/modification of equipment/systems/software.

2. Validation and verification that equipment/systems are operational.

3. In some less common installation scenarios, rack modification may be necessary. This could potentially include removing the back of a rack, disconnecting/reconnecting/rearranging cables, installing rack slides, rearranging rack slides, drilling holes, and using fasteners such as screws to attach hardware.

The contractor shall provide installation testing and logistic support documentation and services as described in this section of the PWS.

3.2.3.2.1 Platform System Operational Verification Testing

The contractor shall provide support to conduct a Platform SOVT utilizing government approved test plans and procedures. This process will include an inspection of the system installation for discrepancies. All discrepancies shall be documented and included in the completed SOVT document (CDRL T009).

The contractor shall perform system checkout/Platform System Operational Verification Tests in accordance with the government approved SOVT document (CDRL T009) for the installation. The contractor shall correct all installation related deficiencies discovered during the Platform SOVT or refer these to the assigned Project Lead for further action. Major discrepancies and/or deficiencies that will adversely impact task completion schedule shall be immediately reported to the assigned Project Lead and government SDM. The contractor shall provide an operational system to be certified by the designated government point of contact, SDM, quality inspector (Contractor QA Lead) and the receiving activity (Ship, Sub, or Shore Site).

3.2.3.2.2 Training Support

The contractor shall conduct on-site training on specific software as part of the installation/upgrade task. The contractor shall record and submit the names and points of contact information for all individuals receiving training, the training dates, and training locations prior to leaving the afloat platform or installation site.

3.2.3.2.3 Installation Logistic Support Documentation

The contractor shall provide recommended changes/modifications to the Platform SOVT and tests, Software Installation Plan (SIP), SAG or other documentation (CDRL T009) as identified by red-lining the document (CDRL T009) in accordance with BA ISEA processes and procedures. At the conclusion of each installation, the contractor shall furnish two copies of modification/red-lined version of the SIP (CDRL T009): one set to the ship, submarine, or shore site upon task completion, and one set to the assigned Project Lead. The red-lined SIP (CDRL T009) shall include the following items:

1. Changes in the Pre-installation procedures for the applications

2. Changes in the Installation procedures for the applications

3. Changes to configuration settings for the applications being installed

4. Changes to environment settings (i.e., hardware, software)

5. Changes to database settings and files

3.2.3.3 Technical Assistance

The contractor shall provide technical assistance directly to shore sites and afloat platforms (ships and submarines) for Casualty Report (CASREP) resolution, fault analysis, testing and/or repair of various installed applications and equipment, as assigned, to restore the units to operational status. The contractor personnel providing technical assistance shall be prepared to travel for onsite assistance within 24 hours of notification. These personnel shall be technically knowledgeable and capable of analyzing system problems and implementing corrective actions without direct assistance or support from NIWC Atlantic personnel when required. The contractor shall submit findings, analysis results, and failure and corrective action reports associated with the technical assistance provided, after issue resolution.

3.2.3.3.1 Fault Isolation and Repair

The contractor shall perform fault isolation and repair on equipment/systems. Faults discovered and corrective action taken shall be documented and conveyed to the COR and assigned Project Lead. If the unit is not repairable or if such repair is outside the scope of the assignment, the Contractor must immediately notify the assigned Project Lead or ISEA and obtain proper instructions for reporting and/or returning the item.

3.3 TECHNICAL SUSTAINMENT SUPPORT (OMN)

Technical Sustainment Support Services within this Task Order (TO) are provided for NIWC Atlantic in support to the PEO MLB LOG IT Services Delivery Team. This support encompasses sustaining the BA ISEA IPT's current solution as well as transitioning and integrating BA ISEA IPT's existing capabilities into the PEO MLB LOG IT Services Delivery Team's future FoS.

The contractor shall provide Technical Sustainment Support services for Distance Support (Service Desk), Documentation Services Support, Proactive Sustainment Support, and Networking Services Support to United States Fleet Forces (USFF) and Foreign Military Services (FMS) customers and end-users by providing timely information and technical assistance.

The contractor shall provide functional Subject Matter Experts (SMEs) with application knowledge and experience required to review, address, and resolve or make recommendations for resolution of incident tickets. (Reference PWS Attachment 1 for specific application information)

Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended workweek (EWW) may be required for professional (i.e., salaried) employees.

3.3.1 Service Desk Services Support

The contractor Service Desk support shall assist with Service Desk activities and act as points of contact (POCs) for the BA ISEA IPT Service Desk. The contractor shall utilize the tiered support process to ensure incident tickets are properly maintained and escalated.

The BA ISEA IPT Service Desk support activities are executed in a blended staff environment to include Civilians, Military, and contractor support personnel. The Service Desk Contractor support provided in this TO shall blend into this Service Desk model and have the knowledge and experience to fill gaps and provide support across the BA ISEA IPT.

The contractor Service Desk support are expected to be co-located with the BA ISEA IPT Service Desk Civilians and Military personnel. However, alternate work locations may be approved by the COR. Alternate work locations are not an option for all positions and personnel due to the work requirements. (Reference section 2.3 of this PWS)

The contractor shall provide Service Desk Services support to assist USFF and FSM customers with incident ticket resolution by providing technical assistance to create, review, process, and track incident tickets through resolution via the NIWC Atlantic's Incident Management tool. Occasionally, after all other distance support options have been exhausted, the contractor may be required to provide on-site technical support to troubleshoot and resolve an incident ticket. On-site technical support locations may be CONUS, OCONUS, or aboard a ship. For on-site visits, the contractor shall provide a Technical Assist Visit Report (CDRL T010).

The BA ISEA IPT Service Desk team is transitioning to Agile processes. The contractor shall work with the team to provide metrics (CDRL T011) in accordance with the BA ISEA IPT processes and procedures.

The contractor shall provide Service Desk support across the BA ISEA IPT to include support for:

1. Operating Systems (OS) (Windows, Linux)

2. OS Security
3. Authentication
4. Access Control
5. Virtualization
6. Troubleshoot applications and communications paths
7. Data replication
8. Database maintenance
9. External/internal environments
10. External/internal interfaces
11. Virtual Private Networks (VPNs)
12. Packet Capturing Analysis
13. Vulnerability Scanning
    - Assured Compliance Assessment Solution (ACAS)
    - Host Based Security System (HBSS)
    - Vulnerability Remediation Asset Manager (VRAM)
14. Encryption
15. Logging

3.3.2 Proactive Sustainment Services

The contractor shall provide support to perform Health Checks (CDRL T012) and Site Visits (CDRL T012) to determine the overall health and functionality of BA ISEA IPT's servers and databases in accordance with the BA ISEA IPT's Proactive Sustainment Policies . The contractor shall perform pre/post-deployment health checks to determine what issues the unit may be having and complete the Health Check form (CDRL T012). If a site visit is required, the contractor shall complete a Site Visit form (CDRL A012) in conjunction with the Health Check Form (CDRL T012). In addition to the Health Check Form (CDRL T012), the contractor shall create incident tickets for issues/problems that arise, to ensure they are tracked through resolution. The contractor shall maintain a Site Status List (CDRL T012).

The contractor shall provide support that have the knowledge and experience to run database cleanup scripts, Top Tier Health Report reviews, and other system and database-related checks.

The contractor shall provide support to document incident tickets to fulfill the metrics gathering (CDRL T011) requirement in accordance with the established processes and procedures, to provide Fleet Readiness Directorate (FRD) program managers (PMs), Fleet Support Teams (FSTs), and ISEAs the ability to monitor performance of the application in their Area of Responsibility (AOR). The contractor support is critical as it provides BA ISEA personnel the ability to identify potential system issues and anomalies quicker resulting in a shorter turnaround time to resolution.

3.3.3 Documentation Services Support

The contractor shall provide support to enter data into the BA ISEA IPT Knowledge Base Database in accordance with the BA Systems Knowledge Base Article Creation Procedure. Knowledge Base (KB) articles (CDRL T013) facilitate service to customers by providing solutions to known issues. The contractor support shall examine the accuracy and integrity of the information and draft KB articles for resolutions for unknown issues and shall publish the KB article (CDRL T013) to KB Database for use.

The contractor shall provide support to assist with creation of Technical Sustainment work instructions (CDRL T014), technical Standard Operating Procedures (SOPs) (CDRL T014), and training documentation (CDRL T014). The contractor support shall review and make recommendations for improvement for existing Technical Sustainment SOPs and training documentation.

The contractor shall assist with drafting Technical Advisories and Fleet Advisory messages.

3.3.4 Networking Services Support

The contractor shall provide support for general network engineering, analysis, and solutions. The contractor shall participate in meetings to identify requirements, obstacles, and solutions.

The contractor shall troubleshoot end-to-end connections between enterprise networks (e.g., NMCI, ONE-Net, MCEN, IT21/CANES). The contractor shall provide phone and email support to customers to resolve network outages. The contractor shall work with customers to resolve network services incident tickets through resolution and closure.

The contractor shall draft and submit Boundary Change Requests (BCRs) (CDRL T015) to update enterprise network firewalls and VPNs.

The contractor shall create and modify network diagrams (CDRL T015) using Microsoft Visio.

3.4 LOGISTICS ENGINEERING SUPPORT (OPN, OMN)

The contractor shall provide logistics engineering support services for acquisition and procurement of supplies and equipment support, technical data maintenance and documentation support, and configuration management of fielded systems support. This support encompasses sustaining the BA ISEA IPT's current solution as well as transitioning and integrating BA ISEA IPT's existing capabilities into the PEO MLB LOG IT Services Delivery Team's future FoS.

3.4.1 Acquisition and Procurement of Supplies and Equipment Support

The contractor shall provide functional and technical expertise to evaluate and translate scheduled installations into approved hardware baselines (CDRL T016) and develop material requirements (CDRL T016) based on the approved baselines and approved installations.

The contractor shall assist with market research and request, receive, and review quotes for accuracy. The contractor shall coordinate with the government materials procurement POC to assist with material procurement artifacts (CDRL T016) through delivery order closeout date. This includes interfacing with vendors to determine estimated delivery dates, product shortages, issues, and replacement of failed or damaged deliveries.

Once the government has acquired the materials, the contractor shall assemble, test, and ship hardware to USFF customers in the field, both ashore and afloat. The contractor shall support provisioning for initial support, sustainment, and end of system life support to include providing material requirements for the government to acquire materials. The contractor shall distribute materials and supplies as required. The contractor shall coordinate with the government to replenish inventories as reflected in the supply support strategy, ensuring spares, repair parts, support tools, materials, and supplies are readily available.

3.4.2 Hardware Engineering Support

The contractor shall provide engineering support that have knowledge and experience with USFF afloat and ashore platforms. The contractor shall be familiar with the internal/external interfaces of the various configurations of afloat systems. The contractor shall provide on-site and distance (phone) technical assistance to USFF customers experiencing hardware failures.

The contractor shall provide support to research and identify replacement equipment (CDRL T017) for hardware.

The contractor shall provide support for testing and evaluation of commercial-off-the-shelf (COTS) equipment. The contractor shall develop Factory Acceptance Tests (FATs) (CDRL T017) and conduct testing of full-rate production racks prior to Fleet installation.

The contractor shall provide support to develop plans, specifications, and requirements documents (CDRL T017). The contractor shall develop detailed instructions for installing and de-installing equipment (CDRL T017). The contractor shall review engineering drawings and assist with revisions and updates. The contractor shall conduct technical oversight and coordination of stakeholder new equipment review/approvals for Naval Sea Systems Command (NAVSEA) Planning Yards, NIWC Atlantic/Pacific, and Naval Undersea Warfare Center (NUWC).

3.4.3 Maintenance of Technical Data and Documentation Support

The contractor shall provide support to develop ILS artifact packages, engineering technical documentation, system nomenclature, and update and maintain the Configuration Management (CM) tool. The Navy is in the process of transitioning its Navy System of Record for CM from Configuration Data Managers Database - Open Architecture (CDMD-OA) to Model Based Product Support (MBPS).

The contractor shall provide support that have knowledge and experience with USFF installations and operations, the Fleet Modernization Process (FMP), and NIWC SOVT Preparation and Execution Guide (SPEG), SPAWARINST 3084.1. The contractor shall be familiar with MIL-STD 196E and shall create system nomenclature using the Joint Electronics Type Designation Automated System (JETDAS).

The contractor shall provide support to conduct requirements analysis and develop, review, revise, and update technical documents in support of hardware and software modifications and upgrades of equipment and systems necessary to operate, maintain, and return equipment or system to a serviceable state.

3.4.3.1 System Operational Verification Test (SOVT)

The contractor shall provide support to develop SOVTs (CDRL T018) in accordance with SPAWARINST 3084.1 and deliver to the government in accordance with the BA ISEA IPT processes, procedures, and timelines.

3.4.3.2 Engineering Change Order (ECO) and Software Delivery Document (SWD)

The contractor shall provide support to develop ECOs (CDRL T018) and SWDs (CDRL T018) in accordance with the NAVWAR Handbook (SPAWARINST 4130.5), and NAVSEA Fleet Modernization Program (FMP) Management and Operations Manual (SL720-AA-MAN-010). The contractor shall develop Installation Procedures for equipment and racks to support the ECOs or Ship Alterations. ECOs (CDRL T018) and SWDs (CDRL T018) shall be delivered to the government in accordance with the BA ISEA IPT processes, procedures, and timelines.

3.4.4 Integrated Logistics Support (ILS) and Lifecycle Support

The contactor shall provide ILS Lifecycle support to review, resolve, and close Service Desk tickets requiring hardware support (e.g., failure, breakage, broken parts, part replacements). The contractor support includes addressing the warranty and software associated with the item(s) in the ticket.

The contractor shall provide support to manage lab assets and spare parts and assist with building Allowance Component's List (ACLs) and Allowance Parts List (APLs).

The contractor shall provide support to create ILS Certifications (CDRL T019) and prepare (i.e., wrap, label) the completed ILS packages for shipment (i.e., FedEx, UPS, USPS) to the customer. The contractor is expected to perform in accordance with Fleet Modernization requirements and Ship Program Managers (SPM) Criteria. The contractor shall compare and verify accuracy of data by distribution of a draft ILS Certification to the COR, Engineering, and Logistics team members for validation and corrections. The contractor shall review and update all ILS Certifications (CDRL T019) as it relates to all Ship Change Document (SCD) and Engineering Changes documents.

The contractor shall review provisioning lists (APLs/ACLs) for ILS certifications in reference to engineering changes, ship control documents, or ship alteration documentation and compare APLs/ACLs to configuration data in certification, SIDs, and CDMD-OA/MBPS work files to ensure agreement.

The contractor shall support the development and submittal of requests to acquire Technical Manual Identification Number (TMIN) assignments in the Technical Data Management Information System (TDMIS), in accordance with the Technical Manual (TM) Revision and Submission SOP dated 17 November 2021 or subsequent TM Revision and Submission SOP updates.

The contractor shall supply and maintain APL, platform information to associate hull to technical manuals in TDMIS to the TMMA for C4I Technical Documentation. The contractor shall make recommendations for improvement of existing or updated engineering documentation, plan and track installations for ILS Certifications, and monitor all USFF production requirements as they relate to ILS Certification development. The contractor shall submit any discrepancies to the COR, CM team and the provisioning team for resolution.

3.4.5 Configuration Management (CM) for Fielded Systems

The contractor shall support all aspects of configuration management. The contractor shall document configuration of all new COTS equipment proposed for inclusion. The contractor shall be familiar with PEO C4I Life Cycle Configuration Management Implementation Manual Version 2.0 and NAVWAR Life Cycle Management Policy (SPAWARINST 4130.3). The contractor shall have the knowledge and experience to execute the work using the NIWC Atlantic configuration management tool Configuration Management Professional (CMPRO). The contractor shall develop and track Hardware Configuration Management Baselines (CDRL T020) using CMPRO. The contractor shall update and maintain configuration records to include procurement in the CMPRO database and ensure data management of installed systems that area operational equipment/systems hardware are consistent and are properly controlled and managed to ensure accurate configuration data needed to resolve issues and problems and meet installation requirements.

3.4.5.1 Navy System of Record for Configuration Management

The contractor shall provide support to develop and submit work-files in Configuration Data Managers Database Open Architecture (CDMD-OA)/Model Based Product Support (MPBS) for afloat and ashore activities in accordance with the FMP Management and Operations Manual

(SL720-AA-MAN-010) and BA ISEA IPT CDMD-OA Work Instructions. The contractor shall process and monitor configuration records in CDMD-OA/MPBS to include adding, changing, and deleting ILS records, and tracking, updating, and maintaining records for inventory and life cycle reviews. The contractor shall provide CDMD-OA/MPBS work-files (CDRL T020), Validation Aids (VALAIDs) (CDRL T020), and Alteration Installation Team (AIT) Verification Reports (CDRL T020) to Configuration Data Managers (CDMs) and the installation team prior to installation. CDMD-OA/MPBS work-files shall be entered in the CDMD-OA/MPBS system in accordance with the BA ISEA IPT schedule.

The contractor shall provide support to perform a CM Gap Analysis (CDRL T020).

3.5 SUSTAINMENT ENGINEERING AND HARDWARE ENGINEERING SUPPORT (OMN)

Sustainment Engineering provides support to fleet customers by providing timely data analysis, development, and implementation of engineering changes and technical advisories through approved enterprise processes relative to customer's service request. The service robustly delivers baseline changes through three subservices to include maintenance engineering, lifecycle engineering, and lifecycle testing.

3.5.1 Maintenance Engineering

The contractor shall provide support to maintain and update concepts, tasks, and criteria for all levels of sustainment during the equipment/system life cycle. The contractor shall maintain documentation such as repair standards, drawings, specifications, test procedures, Planned Maintenance System (PMS) documentation, ILS documentation, APL, and Consolidated Ship's Allowance List (COSAL) as part of Maintenance Engineering Artifacts (CDRL T021) for technical accuracy and adequacy.

The contractor shall provide support to maintain and update maintenance inspection criteria and procedures for repair and overhaul of systems and equipment (CDRL T022), assist in design reviews, and evaluate and validate maintenance actions and frequency including PMS documentation, Technical Feedback Reports (TFBRs), and IA compliance (VRAM).

The contractor shall provide support to build APLs and ACLs for the Edge Devices, Virtual Environment 3 (VE3), and peripherals for both aviation deployments and non-CANES platforms for future capabilities.

3.5.2 Lifecycle Engineering

The contractor shall provide support to collect, analyze, and report performance and maintenance data for C4ISR systems utilizing established operational and maintenance data reporting systems such as the 3M system, CASREPs, Service Desk, Supply System, and Failure Reporting Analysis and Corrective Actions System (FRACAS) to determine reliability, maintainability, and availability (RMA). The contractor shall develop RMA Reports (CDRL T023), Technical Advisories (CDRL T023), and Liaison Access Requests (LARs) (CDRL T023) in accordance with the BA ISEA IPT procedures and processes.

3.6 AFLOAT HARDWARE AND SOFTWARE INDEPENDENT VERIFICATION AND VALIDATION (IV&V) SUPPORT (OMN)

The contactor shall provide this support using the Verification and Validation (V&V) tools implemented and provided by the government. The goal within this TO is to align with Agile and DevSecOps methodologies in order to achieve the Navy’s current initiative for Compile to Combat in 24 hours (C2C24). Agile allows for flexibility in the development processes and DevSecOps applies security as a fundamental part of these transformations. The contractor is expected to integrate with Develop teams as necessary to cooperate within the DevSecOps construct. It is expected that the contactor will require guidance and engage with the Government IV&V lead on a frequent basis who will assist as we transition and integrate into these processes, etc.

The contractor shall provide support to perform IV&V by examining the correctness, completeness, reliability, and maintainability of BA ISEA products (hardware and software) at each step in the established BA ISEA afloat processes.

1. Correctness means the product being evaluated satisfies all hardware and system specification requirements.
2. Completeness signifies all required functions are implemented and all necessary hardware and software products are developed and capable of fully supporting the program lifecycle.
3. Reliability indicates the final product can be expected to perform its intended function without error or failure.
4. Maintainability requires that the products designed facilitate and simplify lifecycle maintenance and modifications.

The contractor shall provide support to report hardware and software issues in accordance with the BA ISEA V&V processes and procedures. The contractor shall provide an independent validation and verification assessment for each Release that results in a Software Test Report (CDRL T025).

The contractor shall be responsible for planning and conducting IV&V for hardware and software to ensure that hardware, software applications, and services meet organizational standards and end-user requirements. The contractor shall perform test planning, test design, and test execution to include hardware tested meets specifications, define and track status, and report defects in the Application Lifecycle Management (ALM) Tool or approved defect tracking tool.

3.6.1 BA ISEA Consolidated IV&V SOP and Documentation

The contractor shall modify the current government BA ISEA IV&V SOP (CDRL T024) to integrate all existing internal and external IV&V and Lifecycle Testing processes and procedures to construct an IV&V SOP that reaches across the BA ISEA, to include hardware testing. The modified IV&V SOP shall be reviewed and updated as required. The BA ISEA IV&V SOP shall address all BA ISEA test activities, test events, defect resolution, and metrics reporting. The BA ISEA IV&V SOP shall address and contain the checklists and templates required to successfully execute the BA ISEA IV&V and Lifecycle Tests.

The contractor shall provide support to document all IV&V activities, which will constitute the specific report generated for each IV&V activity. These IV&V reporting standards, procedures, and templates shall be addressed in the government BA ISEA IV&V SOP. The processes, standards, and procedures shall address how the work is executed and how results are captured, documented, and resolved in accordance with the BA ISEA V&V processes and procedures that will become the BA ISEA IV&V SOP. The goal is to get to automated reporting with testing being executed in JIRA/JAMA or equivalent.

3.6.2 Product Assessment Activities

The contractor shall review the project documentation to assess the degree to which the documents, hardware, and software meet system capabilities and acceptance criteria as reflected in the Requirements Traceability Matrix (RTM). The contractor shall review iteration dependent documentation using guidelines (i.e., checklists) for internal consistency, technical adequacy (e.g., requirements are unambiguous and testable), completeness, traceability to and consistency with higher level documentation, feasibility, and appropriate level of detail.

The contractor shall be familiar with the appropriate checklists before commencing the review. As the product is examined, deviations, deficiencies, and errors shall be documented in accordance with the V&V processes and procedures and the Severity Classification Guide, Table 3-1 below. Therefore, it is expected that the contractor support shall prioritize comments by marking them as such.

The contractor shall participate in the In Process Review meetings (i.e., System Requirements Reviews, Design Reviews, or Readiness Reviews), post government acceptance testing.

Note: In addition to using the below table, the contractor support shall refer to the IEEE 12207 severity standards used in testing.

SEVERITY CLASSIFICATION GUIDE Based on guidance from the Institution of Electrical and Electronics Engineers (IEEE) 12207.2.1997, Annex J (Informative).	
Severity	**Applies if a problem could:**
1	Prevent the accomplishment of an essential capability.
	Jeopardize safety, security, or other requirement designated “critical.”
2	Adversely affect the accomplishment of an essential capability and no work-around solution is known.
	Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known.
3	Adversely affect the accomplishment of an essential capability, but a work-around solution is known.
	Adversely affect technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known.
4	Result in user/operator inconvenience or annoyance, but does not affect a required operational or mission essential capability.
	Result in inconvenience or annoyance for development or maintenance personnel, but does not prevent the accomplishment of responsibilities.
5	Any other defect.

3.6.3 Independent Testing

The contractor shall perform an independent test assessment of the product (e.g., baseline release, patch) as directed by the BA ISEA Government V&V Lead. The contractor shall generate the test plan (CDRL T025), test design (CDRL T025), test suites (CDRL T025), and test procedures (CDRL T025) in preparation for IV&V testing. The contractor shall perform independent testing to validate that the target

system meets its critical requirements. This independent testing will compliment rather than duplicate the developer's testing.

The contractor shall provide the results of independent testing to the BA ISEA Government V&V Lead. The contractor shall submit Incident Reports (CDRL T025) to the BA ISEA Government V&V Lead addressing anomalies detected during independent testing. These Incident Reports should be documented in accordance with the BA ISEA V&V processes and procedures, entered in the BA ISEA configuration management system, Naval Research and Development Establishment (NRDE), and tracked independently by the contractor, through closure. Upon resolution of the anomaly, the contractor shall monitor the implementation and retesting of the fix. The contractor shall perform independent regression testing.

The contractor shall perform Test Data Management activities. Create test data (CDRL T025) and ensure its current prior to executing testing. The contractor shall ensure data files are not corrupt, update test data (CDRL T025) on a regular basis (in accordance with the BA ISEA V&V processes and procedures) to include invalid inputs to test negative scenarios and may include all possible combinations of supported and unsupported formats in test data to ensure that test coverage is maximum.

The contractor shall perform complex functional tests (e.g., those requiring knowledge across multiple applications and domain areas), complex integration tests (e.g., those requiring interfaces with multiple internal and/or external systems), ad-hoc, exploratory and edge-case testing, non-functional testing (e.g., performance testing and load testing), government acceptance testing, and user acceptance testing (i.e., FMC).

The contractor shall perform shipboard testing and validation (i.e., CANES, ARRS, ISNS, ISNS ORT, etc.) to include on-site lab testing.

3.6.4 Audit and Analysis of Metrics

The contractor shall audit the tests, provide an analysis of how the test went (CDRL T025), and provide metrics on the defects (CDRL T025) (e.g., defects found, defect density, defects compared to defects found during development testing).

The contractor shall perform Test Certifications to confirm that reported test results are the actual findings of the tests. Test related tools, media, and documentation will be certified to confirm maintainability and repeatability of tests. This may be performed informally or as part of the Functional Configuration Review.

The contractor shall perform User Documentation Evaluations to examine draft documents during the development process to confirm correctness, understandability, and completeness. Documentation may include user manuals or guides, as appropriate for the project.

The contractor shall attend the acceptance demonstrations and perform walkthroughs to participate in the evaluation processes in which development personnel lead others through a structured examination of a product. The contractor shall assess the developer's review process, product checklists, defined roles of participants, and forms and reports. The contractor shall observe to see if the walkthrough process is well-structured and if issues and action items are recorded and progress monitored. The specific types of walkthroughs the contractor may assess include requirements walkthroughs, walkthroughs of the preliminary design and updates of the design, and source code walkthroughs. These walkthroughs do not include opening the code and looking at it. The contractor shall not engage in the SW Development process.

The contractor shall use software metrics to predict the system's ability to comply with requirements and schedules. The contractor shall review proposed software progress and quality metrics for conformance to the Agile Software Development Lifecycle processes and engineering principles as well as the BA ISEA V&V process and procedure reporting requirements. As the IV&V Agile progression continues, the contractor shall engage with the BA ISEA Government V&V Lead for guidance involving metrics requirements, collection, and reporting specifics (e.g., open defects, defect backlog, average days to close defects, reliability growth, defect density, defect removal percentage, defect leakage or defect detection percentage, defects by domain, root cause of defects, defects by type of user, etc.).

3.6.5 Anomaly and Proposed Change Evaluation

The contractor shall monitor the status of target system anomalies (also known as incidents) and deficiencies to assure the validity of any resultant changes. The contractor shall track and perform trend analyses to determine the number of test-related incidents and provide as input to the DSR. If requested by the BA ISEA Government V&V Lead, the contractor shall review software defects discovered (or outstanding) and report them real time so the issue can be addressed real time. The contractor shall review corrective actions, verify priorities, and confirm the disposition of the change. The contractor shall perform detailed reviews of the anomalies to help verify the correct disposition of system problems. If tasked by the BA ISEA Government V&V Lead, the contractor shall participate in the regression testing of the fixes. In addition, the contractor shall support a Defect Review Board (DRB) if requested by the BA ISEA Government V&V Lead and provide inputs as needed.

The contractor shall also review proposed changes/defects when a revision to the baseline requirements is necessary to enhance or improve the function. The contractor shall review the proposed change requirements for feasibility, accuracy, and completeness, while assessing the impact on the operational system. The contractor shall track the proposed changes through closure.

As part of the anomaly and proposed change assessment, the contractor shall execute the following activities in accordance with the BA ISEA V&V processes and procedures:

1. Perform independent impact assessments concerning the expected operational environment, affected interfaces, feasibility, technical approach, and testability.

2. Provide evaluation of risks.
3. Conduct independent reviews of proposed changes as required.
4. Perform traceability analyses to ensure that all affected documents accurately, correctly, and consistently reflect the approved changes.
5. Conduct an independent review of the resulting design.
6. Monitor regression testing to validate incorporated system changes.

3.7 TRAINING ANALYSIS, DESIGN, DEVELOPMENT AND EVALUATION SUPPORT (OMN)

The contractor shall provide support services to systematically design, develop, and deliver instructional products and experiences, both digital and physical. The contractor shall identify the needs of the IPT by performing research and analysis to identify particular strengths and weaknesses within the most critical areas of the IPT. The contractor shall assess internal and external training requirements that involve maintaining and sustaining the BA ISEA IPT's legacy capabilities as well as transitioning to future capabilities to determine the best course of action (CDRL T026). The BA ISEA IPT's current capabilities must be maintained and sustained through the year 2030, while future capabilities planning is already in progress.

The contractor shall perform an Internal (CDRL T026) and External Training Needs Analysis (CDRL T027) to identify the training and development needs of the IPT functional area staff (i.e., Service Desk, Afloat Installers) as well as identifying the needs of the external/end-users (i.e., USFF, NAVSEA, RMCs). The contractor shall plan, analyze, make recommendations for, and determine training solutions (e.g., video, CBT, over-the-shoulder), and level of immersion.

3.7.1 Internal Training – Ashore and Afloat Legacy Capabilities

The contractor shall work directly with the functional area leads to assess training needs (CDRL T026), determine the impact (CDRL T026), define requirements (CDRL T026), identify solutions (CDRL T026), and develop plans (CDRL T026) to implement the training. Due to the requirement to maintain and sustain the legacy capabilities through 2030, the training needs will continue to evolve. The contractor shall determine best course of action (CDRL T026) for embedding training into the processes (e.g., align training to SW modifications).

3.7.2 External / User-facing Training – Ashore and Afloat Future Capabilities

The contractor shall provide support for planning, analysis, design , and development to work with the developers to assess training needs (CDRL T027), define requirements (CDRL T027), identify solutions (CDRL T027), design (CDRL T027), develop (CDRL T027), and implement training products/solutions (CDRL T027). The contractor shall engage with the development teams to understand the depth and breadth of the capabilities in order to design and develop customer facing training requirements (CDRL T027) (e.g., Computer based training products, Instructional briefings such as Slides, PDFs, and videos, creations/review of application self-help to be embedded inside application). Coding is not expected however, the contractor support shall work together with the software vendor in order to integrate training. The contractor shall determine best course of action (CDRL T027) for embedding training into the processes (e.g., align training to SW modifications).

3.8 CONTRACTOR TRANSITION-IN/OUT (OMN)

The Government anticipates 60-90 days for transition-in and transition out. The objective of this task is to provide migration of current activities performed by the incumbent Contractors to a successor Contractor and may require redesigning the current approaches to align with requirements. Transition entails the transfer of and assumption of responsibility for project documentation, resources, assets, and performance. The transition tasks will ensure uninterrupted operations and sustainment support at the end of the period of performance. At the direction of the Government, the Contractor shall provide accountability for the transition of all on-going activities performed by the incumbent Contractor to a successor Contractor or to the Government or to any supporting third party entities. Transition entails the transfer of responsibility for project documentation, resources, assets, and performance to the designated party. It also includes the implementation and readiness of capabilities necessary for all aspects of performance redesign of current technical and management approaches, assumption of audit reviews and readiness all without disruption in schedule, increased costs, degradation to performance, need for increased Government oversight, or likelihood of unsuccessful performance. The Contractor shall document meetings, attendance of individuals, and development of standard operating procedures as appropriate.

3.8.1 Transition Planning and Management

The Contractor shall develop and execute a Transition Plan (CDRL T028) to ensure an effective, orderly, and efficient execution of both transitioning in and out for either all or a part of the services under this Task Order as directed by the Government. Transition activities include planning, discovery, and programmatic functions (e.g., Contract Management, Human Resource Management, and Quality Assurance) necessary for establishing effective knowledge transfer. Throughout the transition period, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission.

3.8.2 Transition Activity

The Contractor shall transition all active tasks at the time of the transition and all associated system documentation and tools updated to represent the current baseline implementation. Specifically, the Contractor shall:

1. Execute transition activities to ensure continuity of services, minimize any decreases in productivity, prevent degradation of services, and prevent negative impacts to the continuity of care during the transition period.
2. Provide knowledge transfer, support successor job shadowing, training, and other activities in order to successfully transition operation of services.
3. Transfer software licenses to the Government.
4. Deliver all training documentation requested by the Government.
5. Transfer documents, badges, and CACs.
6. Identify and transfer or destroy any classified materials or information IAW Government Security Officer instructions.
7. Deliver all technical data, computer software, and computer software documentation generated in the performance of this contract pursuant to DFARS 252.227-7027.
8. Deliver all commercial and non-commercial technical data, computer software, and computer software documentation not generated in performance of this Task Order that is necessary, as determined by the Government at its sole discretion, to operate and sustain BA ISEA applications throughout its lifecycle.
9. If requested by the Government, export and deliver all data content with context (e.g., schemas, data format, data descriptions, and metadata) in a Government approved common standard electronic machine-readable format.
10. Provide transition progress updates as part of the TOSR (CDRL T001) and during the Program Management Reviews (CDRL T004).
11. Transfer service responsibility at the end of the transition timeframe, upon which the successor Contractor shall assume responsibility for operational, technical, and financial performance.

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

The contractor shall adhere to the following requirements when the IT support services and/or supply are applicable to the requirement:

4.1.1 Ensure that no production systems are operational on any research, development, test and evaluation (RDT&E) network.

4.1.2 Follow DoDI 8510.01 when deploying, integrating, and implementing IT capabilities.

4.1.3 Migrate all Navy Ashore production systems to the Navy, Marine Corps Intranet (NMCI) environment where available.

4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3C and DoDI 8510.01 prior to integration and implementation of IT solutions or systems.

4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on task order in the Department of Defense IT Portfolio Registry (DITPR)-DON.

4.1.7 Ensure all IT products and services recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, Title 36 Code of Federal Regulations Part 1194 – Electronic and Information Technology Accessibility Standards unless otherwise exempt in accordance with the latest regulation.

4.1.8 Only perform work specified within the limitations of the basic contract and task order.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors shall not recommend or purchase commercial software products, hardware, and related services on this task orders.

4.2.1 DoN Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program

The contractor shall not purchase software or software licenses in support of DoN or DoD programs on this task order.

4.2.2 DoN Application and Database Management System (DADMS)

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. The RDT&E network does not provide continuous support to operational entities. The contractor shall ensure that any system achieving operation fleet readiness and support is removed from the RDT&E environment and hosted on the respective enterprise solution as required. The contractor shall ensure any systems or applications integrated, installed, or operated on the RDT&E network must be in accordance with DADMS and/or DITPR-DON registration policies. Exemptions to this policy can apply as specified by higher directives. Exemptions on systems that remain on the RDT&E are normally systems that support the RDT&E or have to be on the RDT&E to achieve their target of support.

4.2.3 Cybersecurity/Computer Security Requirements

The contractor shall ensure that all products recommended and/or procured that impact cybersecurity or Information Assurance (IA) shall be selected from the National Information Assurance Partnership (NIAP) Validated Products List. The contractor shall ensure the products chosen are based on the appropriate NIAP-approved Protection Profile (PP) for the network involved, and are utilized in accordance with latest Defense Information Systems Agency (DISA) policy at time of order. The contractor shall store all product information and have it available for government review at any time.

4.2.4 Supply Chain Risk Management

“Covered item of supply” (e.g., software, processor, etc.) is any information technology item that is purchased for inclusion in a “covered system” (i.e., national security systems). The contractor shall not recommend or purchase products in support of a covered system on this task order.

4.3 CYBERSECURITY SUPPORT

Cybersecurity is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

4.3.1 Cyber IT and Cybersecurity Personnel

4.3.1.1 The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 5239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M and subsequent manual [DoD 8140] when applicable prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the task order performance period or before assignment to the task order during the course of the performance period.

4.3.1.2 Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in Para 8.2.2.4(b).

4.3.1.3 Contractor personnel with privileged access shall have a favorably adjudicated Tier 5 background investigation and acknowledge special responsibilities with a Privileged Access Agreement (PAA) in accordance with SECNAVINST 5239.20A.

4.3.2 Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum: Acceptable Use of Department of the Navy Information Technology (IT) dtd 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in Para 4.2.2.

Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

4.3.3 Cybersecurity Workforce (CSWF) Report

In accordance with DFARS 252.239-7001 and DoD 8570.01-M, the contractor shall identify cybersecurity personnel, also known as CSWF and Cyber IT workforce personnel. The contractor shall develop, maintain, and submit a monthly CSWF Report (CDRL T029) identifying CSWF individuals who are IA trained and certified. Utilizing the format provided in CDRL T029 Attachment 1 of Exhibit A, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Although the minimum frequency of reporting is monthly, the COR can require additional updates at any time. Contractor shall verify with the COR or other Government representative the proper labor category CSWF designation and certification requirements. The primary point of contact (POC) for all related CSWF questions is the Command CSWF Program Manager (PM) in the office of the NIWC Atlantic Information Systems Security Manager (ISSM).

4.3.4 Cybersecurity Workforce (CSWF) Designation

CSWF contractor personnel shall perform cybersecurity functions. In accordance with DoD 8570.01-M Information Assurance Workforce Improvement Program Manual, the CSWF is comprised of the following categories: IA Technical (IAT) and IA Management (IAM)); and specialties: Computer Network Defense Service Providers (CND-SPs) and IA System Architects and Engineers (IASAEs). Based on the IA function provided by the individual, an IA designator is assigned that references an IA category or specialty. The contractor shall have the following quantity of CSWF personnel meeting IA Designator and IA Level/Position requirements:

Labor Category	**Quantity Personnel**	**IA Designator**	**IA Level / Position**	**IA Duty Hours**		
				Primary (=25 hrs)	**Additional (15-24 hrs)**	**Embedded (1-14 hrs)**
Engineer/Scientist 4	1	IAT	Level 2	X		
Engineer/Scientist 5	4	IAT	Level 2	X		
Subject Matter Expert 3	3	IAT	Level 2	X		
Subject Matter Expert 4	1	IAT	Level 2			X
Technical Analyst 1	2	IAT	Level 2		X	
Technical Analyst 2	1	IAT	Level 2		X	
Technical Analyst 2	1	IAT	Level 2			X
Technical Analyst 3	1	IAT	Level 2			X

5.0 TASK ORDER ADMINISTRATION

Administration of the work being performed is required; it provides the Government a means for task order management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government’s requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACTOR LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and COR. The contractor PM, located in the contractor’s facility, shall ultimately be responsible for ensuring that the contractor’s performance meets all Government contracting requirements within cost and schedule. PM shall have the requisite

authority for full control over all company resources necessary for task order performance and be available to support emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate periodic meetings with the COR.

5.2 CONTRACT MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day including business and non-business hours in order to facilitate a timely task order response or modification in particular during urgent requirements.

5.2.1 Task order Administration & Documentation

Various types of administration documents are required throughout the life of the task order. At a minimum, the contractor shall provide the following documentation:

5.2.1.1 Task Order Status Report (TOSR) -- The contractor shall develop a TOSR (CDRL T001) and submit it monthly; the initial report is due at least 30 days after task order award and on the 10th of each month for those months the task order is active. The prime contractor shall be responsible for collecting, integrating, and reporting any subcontractor reports. This CDRL includes the completion of applicable attachment(s) as cited in the DD Form 1423. The contractor shall deliver the TOSR in an editable format; see applicable DD Form 1423 for additional reporting details and distribution instructions.

5.2.1.2 Ad-hoc Status Report/Data Calls – the contractor shall develop and submit a data call report (CDRL T030) which is e-mailed to the COR within 24-48 hours of the request. The contractor shall ensure all information provided is the most current. Cost and funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum, the contractor shall include in the data call the following items and data:

1. Percentage of work completed

2. Percentage of funds expended

3. Updates to the POA&M and narratives to explain any variances

4. List of personnel (by location, security clearance, quantity)

5. Most current GFP and/or contractor acquired Property (CAP) listing

5.2.2 Closeout Report

The contractor shall develop a task order closeout report (CDRL T031) and submit it no later than 15 days before the task order completion date to allow for any corrective actions. The prime contractor shall be responsible for collecting, integrating, and reporting all subcontracting information, if applicable. See corresponding DD Form 1423 for additional reporting details and distribution instructions. The contractor shall ensure with the COR no corrective action is identified, and if corrective action is necessary, the contractor shall rectify issue prior to the end of task order performance period.

5.2.3 WAWF/PIEE Invoicing Notification and Support Documentation

Pursuant to DFARS 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Wide Area Work Flow (WAWF) application (part of the Procurement Integrated Enterprise Environment (PIEE) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. The contractor shall provide e-mail notification to the COR when payment requests are submitted to the WAWF/PIEE and the contractor shall include cost back–up documentation (e.g., delivery receipts, time sheets, & material/travel costs, etc.) to the invoice in WAWF/PIEE. When requested by the COR, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL T032) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.2.4 Electronic Cost Reporting and Financial Tracking (eCRAFT)

The contractor shall complete an Electronic Cost Reporting and Financial Tracking (eCRAFT) Report (CDRL T033) and submit the report on the day and for the same timeframe as when the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. The amounts reported in eCRAFT Periodic Reporting Utility (EPRU) spreadsheet shall be the same reported in WAWF. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination. The contractor shall refer to Attachment #3 eCRAFT Crosswalk and DD Form 1423 for reporting details and upload instructions.

5.2.5 Limitation on Subcontracting

Pursuant to FAR 52.219-14 (DEV 2021-O0008), limitations on subcontracting is applicable for contracts/task orders that have been wholly or partially set aside for small business or 8(a) concerns above the simplified acquisition threshold. To ensure compliance with the applicable FAR Limitation on Subcontracting requirements, the contractor shall develop and submit a Limitation on Subcontracting Report (LSR) (CDRL T034) every 3 months where data collection ending on the last day of the 3-month cycle (average 90-day). Subsequent submissions are due no later than 10 days after the end of the next 3-month period and is an accumulation of the subcontracting efforts to date; see applicable DD Form 1423 for reporting details and distribution instructions. The Government reserves the right to perform spot checks and/or request copies of any supporting documentation.

5.3 CONTRACT PERFORMANCE MANAGEMENT

Contractor performance standards and requirements are outlined in the task order QASP. The ability of a contractor to perform to the outlined standards and requirement will be captured in the Contractor Performance Assessment Reporting System (CPARS). In support of tracking contractor performance, the contractor shall provide the following documents: Cost and Schedule Milestone Plan (CDRL T002) submitted 30 days after task order award and CPARS Draft Approval Document (CDAD) Report (CDRL T035) submitted monthly.

5.4 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this task order does not require Earned Value Management (EVM) implementation due to the majority of efforts on this task order is non-scheduled based (i.e., level of effort) and does not lend itself to meaningful EVM information. In lieu of an EVM system, the contractor shall develop and maintain a Contract Funds Status Report (CDRL T003) to help track cost expenditures against performance.

6.0 DOCUMENTATION AND DELIVERABLES

6.1 CONTRACT DATA REQUIREMENTS LIST (CDRL)

The following listing identifies the data item deliverables required under this task order and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under this task order. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs. The contractor shall not develop any CDRL classified TOP SECRET with Sensitive Compartmented Information (SCI).

Unless otherwise specified, dates are calendar days; one week equals 7 calendar days; 1 days equals 24 hours; and a 24-hour time period is consecutive hours that is exclusive of non-workweek days.

6.1.1 Administrative CDRL

The following table lists all required administrative data deliverables, CDRLs, applicable to this task:

CDRL #	Deliverable Title	PWS Reference Para	Frequency	Date Due
T001	Task Order Status Report (TOSR)	3.1.1.1, 3.1.2.1, 3.1.4, 3.8.2, 5.2.1.1, 8.1.2, 8.2.3.1, 10.0	MTHLY	30 DATO and monthly on the 10th
T002	Cost and Schedule Milestone Plan	3.1.2.1, 3.1.3.1, 5.3	One time with revisions (ONE/R)	NLT 30 DATO; revision NLT 7 days after receipt of Govt review
T003	Contract Funds Status Report (CFSR)	3.1.3.1, 5.4	MTHLY	30 DATO and monthly on the 10th
T029	Cybersecurity Workforce (CSWF) Report	4.3.3, 8.1.2, 8.2.3.1	MTHLY	30 DATO and monthly on the 10th
T030	Data Call Report	5.2.1.2	ASREQ	Within 24-48 hrs after request

CDRL #	Deliverable Title	PWS Reference Para	Frequency	Date Due
T031	Closeout Report	5.2.2, 8.2.2.3	1TIME	NLT 15 days before completion date
T032	Invoice Support Documentation	5.2.3	ASREQ	Within 24 hrs from request
T033	Electronic Cost Reporting and Financial Tracking (eCRAFT) Report	5.2.4	ASREQ	Same date when invoice is submitted to WAWF
T034	Limitation on Subcontracting Report	5.2.5	TRI-MTHLY	NLT 90 DATO and every third month on the 10th
T035	Contractor CPARS Draft Approval Document (CDAD) Report	5.3	MTHLY	30 DATO and monthly on the 10th
T036	OCONUS Deployment Package	11.3.1	ASREQ	NLT 30 days prior to travel

6.1.2 Technical CDRL

The following table lists all required technical data deliverables, (CDRLs), applicable to this task order:

CDRL #	Deliverable / SubTitle	PWS Reference Para	Frequency	Date Due
T004	Status Report / Program Management Reviews (PMRs)	3.1.2.1, 3.1.3.1, 3.1.4, 3.1.6, 3.8.2	MTHLY	30 DATO and monthly on the 10th
T005	Installation Planning Artifacts	3.2.1	ASREQ	NLT 60 days prior to install
T006	Database Conversion POA&Ms (Build & QA)	3.2.2	MTHLY	30 DATO and monthly on the 10th
T007	Daily Status Reports (DSRs)	3.2.3	ASREQ	Within 24-hours of installation
T008	Pre-installation Artifacts	3.2.3.1	ASREQ	Within 7 days of installation
T009	Installation Red-lined Artifacts	3.2.3.2.3	ASREQ	Within 7 days of installation

CDRL #	Deliverable / SubTitle	PWS Reference Para	Frequency	Date Due
T010	Technical Assist Visit Report	3.3.1	ASREQ	Within 7 days of Visit
T011	Service Desk Metrics	3.3.1	MTHLY	30 DATO and monthly on the 10th
T012	Health Check & Site Visit Artifacts	3.3.2	ASREQ	Within 7 days of check/visit
T013	Knowledge Base Articles	3.3.3	ASREQ	Within 7 days of receiving
T014	Technical Sustainment SOPs and Training Documentation	3.3.3	ONE/R	NLT 30 DATO; revisions NLT 7 days after receipt of Govt review
T015	Networking Services Artifacts	3.3.4	ASREQ	Within 7 days of request
T016	Supplies and Equipment Artifacts	3.4.1	ASREQ	Within 7 days of request
T017	HW Engineering Data & Technical Artifacts	3.4.2	ASREQ	Within 7 days of request
T018	Technical Data & Documentation Artifacts	3.4.3.1, 3.4.3.2	ASREQ	Within 7 days of installation
T019	ILS Certification Artifacts	3.2.1, 3.4.4	ASREQ	Within 7 days of installation
T020	CM Artifacts	3.4.5, 3.4.5.1	MTHLY	90 DATO and monthly on the 10th
T021	Maintenance Engineering Artifacts	3.5.1	MTHLY	30 DATO and monthly on the 10th
T022	Maintenance Inspection Criteria and Procedures	3.5.1	MTHLY	30 DATO and monthly on the 10th
T023	Lifecycle Engineering Artifacts	3.5.2	ASREQ	Within 7 days of request
T024	BA ISEA IV&V SOP	3.6.1	ASREQ	Within 60 Days of COR request

CDRL #	Deliverable / SubTitle	PWS Reference Para	Frequency	Date Due
T025	IV&V Testing Artifacts	3.6, 3.6.2, 3.6.3, 3.6.4	ASREQ	Per IV&V Schedule
T026	Internal Training Artifacts	3.7.1	MTHLY	30 DATO and monthly on the 10th
T027	External Training Artifacts	3.7.2	MTHLY	30 DATO and monthly on the 10th
T028	Transition Plan	3.8.1	2TIMES	First NLT 21 DATO; Final NLT 120 days before TO completion date
T037	Navy Shipboard/Submarine Safety Documentation	12.1.1	ONE/R	NLT 30 DATO; revisions NLT 7 days after receipt of Govt review
T038	Test and Inspection Plan (TIP)	7.2.2.1	ASREQ	Within 7 days of installation
T039	Test and Inspection Results	7.2.2.2	ASREQ	NLT 7 days after completion of installation

6.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, and etc., are provided in a format approved by the receiving Government representative. The contractor shall provide data in an editable format compatible with NIWC Atlantic corporate standard software configuration as specified below or as directed by the COR (e.g., DSRs – CDRL T007). Contractor shall conform to NIWC Atlantic corporate standards within 30 days of task order award. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.*

	Deliverable	Software to be used
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher/FrameMaker
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint

	Deliverable	**Software to be used**
e.	3-D Drawings/ Graphics/Schematics (new data products)	SolidWorks, Creo, or Inventor
f.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
g.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
h.	Scheduling	Microsoft Project
i.	Computer Aid Design (CAD) Drawings and Network Diagrams	AutoCAD/Microsoft Visio
j.	Geographic Information System (GIS)	ArcInfo/ArcView
k.	On-line Training Development	Adobe Captivate

6.3 INFORMATION SYSTEM COMMUNICATION

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. As required, prior to CDRL submission due date, the contractor shall establish necessary access to the Government IS by utilizing an employee issued Common Access Card (CAC) and/or DoD approved External Certification Authority (ECA) (https:// public.cyber mil/eca/). The contractor shall be capable of Public Key Infrastructure (PKI) client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on task shall be accessible by e-mail through individual accounts during all hours. The contractor shall have an information system capable of meeting all security requirements identified under Para 8.4.

7.0 QUALITY

7.1 QUALITY SYSTEM

Upon task order award, the prime contractor shall have and maintain a quality system that meets contract and task order requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The contractor shall have an adequately documented quality system which contains processes, procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system, which includes an internal auditing system. The contractor shall make their quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this task order may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan or quality system, and development of quality related documents. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

(i) Establish documented, capable, and repeatable processes

(ii) Track issues and associated changes needed

(iii) Monitor and control critical process, product, and service variations

(iv) Establish mechanisms for feedback of field product and service performance

(v) Implement and effective root-cause analysis and corrective action system

(vi) Establish methods and procedures and create data used for continuous process improvement

7.2 MANAGE QUALITY COMPLIANCE

7.2.1 General

The contractor shall have quality processes or a Quality Management System (QMS) in place that coincide with the Government's Manage Quality processes which address Quality Control, Quality Assurance, Software Quality, and/or project Quality System tasks. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288:2015 for System life cycle processes and ISO/IEC 12207:2017 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in Acquisition Milestones, Phases, and Decision Points, which are standard elements of the Defense Acquisition System and support DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment and objective evidence of Lean Six Sigma, Risk Management, and System Engineering methodologies; and System and Software Engineering best practices.

7.2.2 Navy Shipboard/Submarine work

The contractor shall ensure the quality of all services provided under this task order shall be compliant to ISO 9001 in the relevant profession, trade or field of endeavor. Within 30 days of award, the Prime contractor shall have in place, an existing Government approved QMS by the NAVSEA Quality Programs and Certification Office (04RP office) for shipboard and submarine work pursuant to NAVSEA Technical Specification 9090-310 series as applicable. The documented QMS will be used to ensure that the end product of and services associated with each task conforms to contract and task order requirements whether produced by the contractor or provided by approved subcontractors or vendors. The QMS will provide for control over all phases of the various types of tasks, from initial manning and material ordering to completion of final tasking, before offering to the Government for acceptance as specified in this task order PWS. The contractor shall ensure all services are rendered accordingly to the documented QMS, and personnel are directly supervised by individuals qualified in the relevant profession or trade. The contractor shall ensure the QMS addresses the development of the following test and inspection documentation in accordance with NAVSEA Standard Item 009-04:

7.2.2.1 The contractor shall develop and submit to the COR and if applicable the designated QA representative a Test and Inspection Plan (TIP) (CDRL T038) no later than five working days prior to start of productive work on ship/submarine. If the TIP requires a constructive change or error correction as noted by either the contractor or Government, the contractor shall submit a revised TIP (CDRL A038) to the COR and if applicable the designated QA representative no later than 5 days after the identification or notification of the change/error; see applicable DD Form 1423 for additional reporting details and distribution instructions.

7.2.2.2 At the completion of the test, the contractor shall develop and submit to the COR and if applicable the designated QA representative, the Test and Inspection Results (CDR T039) no later than seven days after completion of each applicable test. Any deviation to the time allowance for submittal should be agreed upon between Government and contractor prior to start of test; see applicable DD Form 1423 for additional reporting details and distribution instructions.

7.2.3 Navy Shore work

The contractor shall ensure the quality of all services provided under this task order conforms to high standards, such as ISO 9001 in the relevant profession, trade or field of endeavor. At a minimum, the contractor shall provide services in accordance with the SPAWAR Shore Installation Process Handbook (SPAWAR SIPH). Within 30 days of award, the prime contractor shall have in place, an existing Government approved QMS by the project Quality representative.

7.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified in the contractor‘s Quality Assurance Plan (QAP) or by the respective WBS, POA&M, or quality system/QMS documentation in support of continuous improvement. The contractor shall deliver related QAP and any associated procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes, products, and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related products, services, documents, and material in a category when noncompliance is established.

7.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified in the contractor QAP or by the respective WBS, POA&M, or quality system/QMS documentation.

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

8.0 SECURITY

8.1 ORGANIZATION

8.1.1 Security Classification

As specified in the DoD Contract Security Classification Specification, DD Form 254, the contractor shall perform classified work under this task order. Prior to commencement of classified work, the contractor shall have a SECRET facility clearance (FCL).

8.1.1.1 U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and work within restricted areas unescorted. Access to SCI is limited to U.S. Government Facilities or other U.S. Government sponsored controlled space as authorized on the DD254. The contractor shall not generate any SCI deliverables.

8.1.1.2 This task order requires for various levels of vetting to support specific PWS tasks. The following table outlines the minimum required security clearance per task. The contractor shall provide personnel meeting the specific minimum personnel clearance (PCL) for access to support the PWS tasks listed below:

Required Security Clearance	**PWS Task Paragraph**
Secret	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or access to Government facility/installation and/or access to information technology systems under this task order. The FSO is typically a key management person who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this task order. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on task order. Responsibilities include tracking all personnel assigned Government Common Access Card (CAC) and NIWC Atlantic badges (issuances and expiration dates) and entering/maintaining personnel security mandatory training information within the Staffing Plan document, which is an attachment to the TOSR (CDRL T001) including updating and tracking data in the CSWF Report (CDRL T029). The FSO shall ensure the latest NIWC Atlantic Contractor Check-in and Check-out (CICO) procedures are implemented and followed.

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30C, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on this task order, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the task order and are certified/credentialed for the CSWF. A favorable background determination is determined by either a Tier 1 (T1) investigation, Tier 3 (T3) investigation, or Tier 5 (T5) investigation and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or NIWC Atlantic information. *Cost to meet these security requirements is not directly chargeable to task order.*

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum security requirements, the contractor shall permanently remove the individual from NIWC Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied," receives an "Interim Declination," or unfavorable fingerprint, the contractor shall remove the individual from NIWC Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task orders.

8.2.1 Personnel Clearance

All personnel associated with this task order shall possess a SECRET personnel security clearance (PCL) for access. These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data to include having access to Naval Nuclear Propulsion Information (NNPI) Data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the DoD CAF and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Any future revision to the respective directive and instruction will be applied as a task order modification. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance

with appropriate Department of Defense, Navy, and NIWC Atlantic security regulations. The contractor shall immediately report any security incident or insider threat indicator to the NIWC Atlantic Security Management Office, the COR, and Government Project Manager.

8.2.2 Access Control of Contractor Personnel

The contractor shall facilitate the required access for each employee. The ability of the contractor to manage and maintain accessibility in accordance with the applicable requirements is captured in the annual Government CPARS rating.

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities/installations require a CAC for access. Contractor personnel shall carry proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement for any liability issues. For admission to NIWC Atlantic facilities/installations, all contractor personnel must have the COR or Government sponsor initiate access. For contractor personnel requiring a Confidential, Secret, or TS security clearance, a visitor authorization request (VAR) must be submitted via Defense Information System for Security (DISS) to the applicable Security Management Office (SMO). The contractor shall send VAR to SMO 652366. If faxing a VAR versus using DISS, the contractor shall submit their request on company or agency letterhead to (843)218-4045 for Charleston or (757)541-5860 for Tidewater locations. For visitation to all other Government locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office.

Joint Personnel Adjudication System (JPAS) is being replaced by DISS. The contractor shall ensure they are capable of accessing DISS when JPAS is no longer accessible. After DISS transition date, contractor shall submit all VARs through DISS.

(b) Contractor employees who make repeated deliveries to JB Charleston military installations and do not require access into NIWC Atlantic facilities or access to IS shall obtain a base access card. Only contractor employees that are able to obtain a card will be eligible for entrance on base. At Joint Base (JB) Charleston, the contractor shall obtain the required access card via the Defense Biometric Identification System (DBIDS) from the JB Charleston Badge and Pass Office. Contractors with employees that that are no longer employed shall return the employee's access card directly to the COR or to the local NIWC Atlantic Security Office with COR notification within five (5) days from the last day of employment. Contractors who do not have a DBIDS card or CAC will receive a one-day pass for each day access is required. Information about DBIDS is found at https://dbids-global.dmdc mil/enroll#!/.

(c) All contractor persons engaged in work while at a Government facility/installation shall be subject to inspection of their vehicles, identification cards, and bags/parcels at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location.

(d) The contractor shall notify the COR and appropriate NIWC security personnel within 24 hours from the time contractor employee gives notice of departure or are removed unexpectedly from contract support. For contractors in direct support of NIWC Atlantic, see the Contractor Check-in and Check-out (CICO) Procedures requirements listed in Para 8.2.2.5.

8.2.2.2 Identification and Disclosure Requirements

All contractor and subcontractor employees located on and off Government installations shall take all means necessary to not represent themselves as Government employees. All contractor personnel shall follow the identification and Government facility disclosure requirement:

(a) Contractor employees shall be clearly identifiable as a contractor while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors shall identify themselves as contractors or subcontractors during meetings, on attendance meeting list/minutes, at the beginning of telephone conversations, in electronic messages including their electronic digital signature, and all correspondence related to this task order.

(c) Contractors occupying facilities within Department of the Navy or other Government installations (such as offices, separate rooms, or cubicles) shall clearly display and identify their space with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

8.2.2.3 Government Badge Requirements

Depending on access required, contractor personnel shall require a Government-issued picture badge. While on Government installations/facilities, contractors shall abide by each site's latest security badge requirements and prominently display (above the waist) their Government-issued picture badge. Government installations/facilities are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards.

(a) Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, etc.) to the applicable Government security

office via the COR who will validate the need authorizing contractor performance within the applicable Government installation/facility.

(b) The contractor shall assume full responsibility for the proper use and security of the identification badge and is responsible for returning the badge upon termination of personnel or expiration or completion of the task order.

(c) The contractor (FSO if applicable) shall track all personnel (including subcontractors) holding CAC and/or NIWC Atlantic Government badges in support of this task as part of the TOSR. At the completion of the task order, the contractor shall provide a list as part of the Closeout Report (CDRL T031) of all returned and unreturned badges with a written explanation for any missing badges.

8.2.2.4 Common Access Card (CAC) Requirements

Contractors supporting work that requires access to Government facilities/installations and/or access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoDM 1000.13-V1, issuance of a CAC is based on the following four criteria:

1. Eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD federally controlled facilities on behalf of the NIWC Atlantic on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
2. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS).
3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoDM 5200.02 – at a minimum, the completion of FBI fingerprint check with favorable results and submission of a T1 investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. Contractor personnel shall contact the NIWC Atlantic Security Office to obtain the latest CAC requirements and procedures.
4. Verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a PKI. A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the task order specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Atlantic Information Systems Security Management (ISSM) office:

1. For annual DoD Cybersecurity/IA Awareness training, the contractor shall use this site: https://mytwms.dc3n.navy.mil/. For contractors requiring initial training and do not have a CAC, contact the NIWC Atlantic ISSM office at phone number (843)218-6152

or e-mail questions to NIWCLANT.ISSM.OPS.FCT@navy.mil for additional instructions. Training can be taken at the ISSM office or online at https://public.cyber mil/training/cyber-awareness-challenge/.

2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form and shall initiate a CAC request via the latest Contractor Check-in procedures as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website at https://www.public navy.mil/navwar/atlantic/pages/contractorcheckin.aspx.

8.2.2.5 Contractor Check-in and Check-out (CICO) Procedures

All NIWC Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a NIWC Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out (CICO) procedures, instructions, and forms as posted on the NIWC Atlantic Command Operating Guide (COG) website or the NIWC Atlantic Public website (under “Contact” tab, select “Contractor Check-In”). In accordance with the monthly status reporting requirements, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this task order within the required timeframe as cited in the CICO instructions. The contractor (FSO, if applicable) shall have IT access to NIWC Atlantic systems for purposes of meeting CICO personnel requirement. For contractor employees whose services are no longer required, the contractor shall ensure all those employees return all applicable Government credentials (keys, CAC, site badges, tokens, etc.) and any assigned Government-furnished property (e.g., laptops) are returned to the COR or appropriate Government representative. The contractor shall ensure all procedures as cited in the Contractor Check-out COG page are followed which includes a completed Contractor Check-out checklist form (SPAWARSYSCEN 5500/3) is submitted for each employee as applicable.

8.2.2.6 Accessing Navy Enterprise Resources Planning (ERP) System

Contractor personnel shall not access the Navy Enterprise Resource Planning (Navy ERP) system.

8.2.3 Mandatory Training

In addition to training requirements and certifications required for a specific labor category, certain contractor personnel (including subcontractors) regardless of security classification shall complete required mandatory training in accordance with NAVWARSYSCOM Code 80330 mandatory training webpage: https://wiki.spawar.navy.mil/confluence/x/jwDsAQ. Contractors without access to the training webpage shall coordinate with the COR concerning the latest mandatory training as specified on the training webpage. The following table is a sample of contractor mandatory training that is subject to change in accordance with the NAVWARSYSCOM website or SECNAVINST:

#	**Training Course Name**	**Contractor Personnel Applicability**
1	Active Shooter, Level 1	All contractors
2	Operations Security (OPSEC)	All contractors
3	Antiterrorism Training, Level 1	Contractors requiring routine physical access to federally controlled facilities or military installations (DFARS 252.204-7004)
4	[NIWC Atlantic] Annual Security Refresher	All fulltime/partial, onsite contractors
5	Suicide Prevention Training (Suicide Awareness)	All fulltime, onsite contractors
6	Records Management	All contractors NMCI account holders

7	DoD Cyber Awareness Challenge	All contractors NMCI account holders and Personnel accessing CAC-enabled government sites – Authorized users of DOD information systems and networks
8	Privacy and Personally Identifiable Information (PII) Awareness Training	All contractors with access to PII
9	NIWC Intelligence Oversight	All contractors
10	Sensitive Compartmented Information (SCI) Initial/Refresher Training	Contractors that are SCI cleared personnel and authorized users of DOD IS and networks

8.2.3.1 The contractor shall be responsible for verifying applicable personnel receive all required training within the specified due dates. The contractor shall track and annotate all mandatory training required and completed for each employee in the Staffing Plan which is part of the monthly TOSR (CDRL T001). For CSWF, contractor shall ensure all mandatory cybersecurity training and certifications are reported in the CSWF Report (CDRL T029).

8.2.3.2 Unless otherwise noted, the contractor shall complete mandatory training annually between 1 October and 30 September utilizing the Total Workforce Management System (TWMS). For some personnel, attendance of Government face-to-face training is allowed if COR concurs with training schedule. For training taken via Defense Information Systems Agency / Navy Knowledge Online (DISA/NKO), the contractor shall forward a copy of the certificate to ssclant_mandatory_tr fcm@navy.mil who will upload or ensure each completed training is recorded in TWMS.

8.2.3.3 The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

8.2.4 Accessing Government Information Systems and Nonpublic Information

Contractor personnel shall meet the following cybersecurity and personnel security requirements when accessing Government information systems and nonpublic information.

Definition – For the purposes of this section, “sensitive information” includes the following:

(a) all types and forms of confidential business information, including financial information relating to a contractor’s pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;

(b) source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 2101-2107);

(c) information properly marked as “business confidential,” “proprietary,” “procurement sensitive,” “source selection sensitive,” or other similar markings;

(d) other information designated as sensitive by NIWC Atlantic and the program.

8.2.4.1 In the performance of the task order, the contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include “sensitive information” or other information not previously made available to the public that would be competitively useful on current or future related procurements.

8.2.4.2 Contractor personnel shall protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the task order, whether the information comes from the Government or from third parties. The contractor shall provide the following support:

(a) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the task order, and not for any other purpose unless authorized;

(b) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the task order or as authorized by Federal

statute, law, or regulation;

(c) Inform authorized users requiring access in the performance of the task order regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.

(d) Execute a “Contractor Access to Information Non-Disclosure Agreement,” and obtain and submit to the Contracting Officer a signed “Contractor Employee Access to Information Non-Disclosure Agreement” for each employee prior to assignment.

(e) Notify the Contracting Officer in writing of any violation of the requirements in Para 8.2.4.2(a) through Para 8.2.4.2(d) as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

8.2.4.3 In the event that the contractor inadvertently accesses or receives any information marked as “proprietary,” “procurement sensitive,” or “source selection sensitive,” or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

8.2.4.4 The requirements of this text are in addition to any existing or subsequent OCI requirements which may also be included in the task order, and are in addition to any personnel security or Information Assurance requirements, including SAAR-N form (DD Form 2875), annual Cybersecurity training certificate, Questionnaire for Public Trust form (SF85P), or other forms that may be required for access to Government Information Systems.

8.2.4.5 Subcontracts. The contractor shall insert Para 8.2.4.1 through 8.2.4.4 in all subcontracts that may require access to sensitive information in the performance of the task order.

8.2.4.6 Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the “Contractor Non-Disclosure Agreement,” a mitigation plan for Government approval, which shall be incorporated into the task order. At a minimum, the mitigation plan shall identify the contractor’s plan to implement the requirements of Para 8.2.4.2 and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the task order from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A “firewall” may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

8.2.5 Handling of Personally Identifiable Information (PII)

In accordance with the Privacy Act of 1974, the contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of Personally Identifiable Information (PII) in accordance with the latest DoN policies. The contractor shall not store any Government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in the header and footer of each page of the document: “CUI”. In addition to marking documents at the top and bottom with “CUI” a CUI “Designation Indicator Block” is required at the bottom of the document’s first page within the “CUI” banner and footer markings. DoD guidance directs that this block be located at the lower right of the page. Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Once notified, the Contracting Officer shall immediately contact the Privacy Act Coordinator. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel. If a contractor, including any subcontractor, is authorized access to PII, the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act.

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. OPSEC requirements are applicable when contract personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, NIWC Atlantic’s OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual and SPAWARSYSCENLANTINST 3070.1B.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall develop their own internal OPSEC program specific to the task order and based on NIWC Atlantic OPSEC requirements. At a minimum, the contractor’s program shall identify the current NIWC

Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial OPSEC training within 30 days of task order award and annual OPSEC awareness training in accordance with requirements outline in the Mandatory Training, Para 8.2.3. OPSEC training requirements are applicable for personnel during their entire term supporting this NIWC Atlantic task order.

8.3.3 NIWC Atlantic OPSEC Program

Contractor shall participate in NIWC Atlantic OPSEC program briefings and working meetings, and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified task order shall have specific OPSEC requirements listed on the DD Form 254.

8.4 INFORMATION SYSTEM SECURITY

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on task. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the task order, and privileged task order information (e.g., program schedules and task order-related tracking).

8.4.1 Hardware and Software

The contractor shall scan all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect task order related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure Data-at-Rest encryption technology is installed on all portable electronic devices including storage of all types.

8.4.2 Safeguards

The contractor shall protect Government information and shall be able to provide documentation (e.g., Systems Security Plan (SSP)) validating they are complying with the requirement in accordance with DFARS 252.204-7012. Subcontractors are subject to DFARS requirements only when performance will involve operationally critical support or covered defense information. The contractor and all applicable subcontractors shall abide by the following safeguards:

8.4.2.1 Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

8.4.2.2 Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

8.4.2.3 Sanitize media (e.g., overwrite, reformat, or degauss) before external release or disposal.

8.4.2.4 Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

8.4.2.5 Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

8.4.2.6 Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g.,

spreadsheet and word processing files), using at least application-provided password protection level encryption. The contractor shall encrypt or digitally sign all communications for authentication and non-repudiation.

8.4.2.7 Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

8.4.2.8 Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

8.4.2.9 Provide protection against computer network intrusions and data exfiltration, minimally including the following:

(a) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

(b) Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(c) Prompt application of security-relevant software patches, service packs, and hot fixes.

8.4.2.10 As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

8.4.2.11 Report loss or unauthorized disclosure of information in accordance with contract, task order, or agreement requirements and mechanisms.

8.4.2.12 Pursuant to DFARS 252.204-7009, the contractor shall not use or disclose third-party contractor reported cyber incident information. The contractor can be held liable for breach of information and shall extend restriction in subcontracts for service that include support to Government’s activities related to safeguarding covered defense information and cyber incident reporting.

8.4.2.13 As applicable, follow minimum standard in SECNAVINST 5510.36B for classifying, safeguarding, transmitting, and destroying classified information and CUI.

8.4.3 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

8.4.4 Covered Defense Information

The contractor shall identify all covered defense information, as defined in DFARS 252.204-7012, and apply markings when appropriate to all deliverables in accordance with DoDI 5200.48.

8.4.5 Utilization of a Government-owned and Government-controlled computer asset

The contractor shall meet specific operational requirements when utilizing a Government-owned computer or Government-controlled software image for a contractor-owned computer (including laptop) that is issued as either an NMCI asset, Government Furnished Property (GFP), or Government Controlled Equipment (GCE). At a minimum, contractor personnel shall comply with the following requirements when utilizing a Government-owned or Government-controlled computer:

8.4.5.1 All messages sent to/from utilize Virtual Private Network (VPN) connections.

8.4.5.2 All messages sent to/from are encrypted.

8.4.5.3 No storage of data on non-compliant networks (e.g., contractor’s corporate systems).

8.4.5.4 Only government email (NMCI, mail.mil, etc.) is allowed to be used; absolutely NO Gmail, other personal systems, and NO corporate email that does not reside on NIST compliant systems shall be utilized.

8.4.5.5 All email must be sent between compliant systems – e.g., sending encrypted email to a private corporate account that resides on an uncompliant network, then decrypting and utilizing it is not allowed.

8.4.5.6 All stored information meets data-at-rest encryption standards – if using GFP, then use the same methods as networked devices (e.g., MS Bitlocker, Symantec Endpoint Security, etc.)

8.4.5.7 All data is housed on GFE shared storage location – ensures government can retrieve its data at any time.

8.4.5.8 In regard to processing, storing, or transmitting CUI, no CUI is allowed on an information system not meeting configuration and security standards.

8.5 ENHANCED SECURITY CONTROLS

Controlled unclassified information (CUI), as defined in DoDI 5200.48, is applicable to this contract. Pursuant to DFARS 252.204-7012, prior to the processing, storing, or transmitting of CUI on an unclassified information system and IT asset that is owned, or operated by or for the contractor, the contractor shall meet the following enhanced security controls.

8.5.1 Systems Security Plan and Plan of Action and Milestones (SSP/POA&M) Reviews

8.5.1.1 Within thirty (30) days of task order award, the contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in DFARS 252.204-7012, which is included in this task order. The contractor shall fully cooperate in the Government's review of the SSPs at the contractor's facility.

8.5.1.2 If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS 252.204-7012 then the Government will notify the contractor of each identified deficiency. The contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The Contracting Officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the contractor to submit a plan of action and milestones (POA&M) for the correction of the identified deficiencies. The contractor shall immediately notify the Contracting Officer of any failure or anticipated failure to meet a milestone and provide an updated POA&M.

8.5.1.3 Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the contractor's facility. The Government may continue to conduct follow-on reviews until the Government determines that the contractor has corrected all identified deficiencies in the SSP(s).

8.5.1.4 The Government may, in its sole discretion, conduct subsequent reviews at the contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of task order award) and may conduct such reviews at any time upon thirty (30) days' notice to the contractor.

8.5.2 Compliance to NIST 800-171

8.5.2.1 The contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&M that varies from NIST 800-171 only in accordance with DFARS 252.204-7012(b)(2), for all covered contractor information systems affecting this task order.

8.5.2.2 Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

(a) Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as Computer Numerical Control (CNC) equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

(b) Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

(c) Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods;

(d) Audit user privileges on at least an annual basis;

(e) Implement:

1. Control 3.13.11 (FIPS PUB 140-2 validated cryptology or implementation of National Security Agency (NSA) or NIST approved algorithms (i.e. FIPS PUB 140-2 Annex A: Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) or compensating controls as documented in a SSP and POA&M); and,

2. NIST Cryptographic Algorithm Validation Program (CAVP)

(see https://csrc nist.gov/projects/cryptographic-algorithm-validation-program);

(f) Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POA&M for implementation which shall be evaluated by the Navy for risk acceptance;

(g) Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

8.5.3 Cyber Incident Response

8.5.3.1 The contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the task order that the contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

8.5.3.2 Incident data shall be delivered in accordance with the DOD Cyber Crimes Center (DC3) Instructions for Submitting Media available at http://www.acq.osd mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx. In delivery of the incident data, the contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

8.5.3.3 If the contractor subsequently identifies any such data not previously delivered to DC3, then the contractor shall immediately notify the Contracting Officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the contractor may request a delivery date later than ten (10) days after identification. The Contracting Officer will approve or disapprove the request after coordination with DC3.

8.5.4 Naval Criminal Investigative Service (NCIS) Outreach

The contractor shall engage with Naval Criminal Investigative Service (NCIS) industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

8.5.5 NCIS/Industry Monitoring

8.5.5.1 In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the contractor shall cooperate with the NCIS, which may include cooperation related to: threat indicators; pre-determined incident information derived from the contractor's infrastructure systems; and the continuous provision of all contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

8.5.5.2 If the Government determines that the collection of all logs does not adequately protect its interests, the contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the contractor. In the alternative, the contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the contractor.

8.5.5.3 In all cases, the collection or provision of data and any activities associated with this PWS shall be in accordance with federal, state, and non-US law.

9.0 GOVERNMENT FURNISHED INFORMATION (GFI)

For the purposes of this task order, Government Furnished Information (GFI) includes manuals, technical specifications, software, software licenses, maps, building designs, schedules, drawings, test data, etc. provided to contractors for performance on this task order. Depending on information contained in a document, the contractor shall comply with additional controls (e.g., completion of a Non-Disclosure Agreements, etc.) for access and distribution. The Government will mark any CUI which includes unclassified covered defense information and unclassified controlled technical information provided to the contractor. For any missing markings, contractor shall request appropriate marking from the Government.

GFI is utilized on this task order. Any applicable document (PWS Para 16.0) not available online, the Government will provide document as GFI listed in the table below. The contractor shall inventory all GFI by tracking distribution and location and provide a GFI inventory to the Government. The contractor shall use the GFI provided to support this task order only – use of GFI document(s) to support other projects beyond this task order is not allowed. Unless otherwise specified, all GFI will be provided by the Government by the estimated delivery date listed in the table below, and the contractor shall return all GFI to the Government at completion of the task order. If a contractor requires additional GFI other than what is listed, the contractor shall submit a request to the COR within 30 days after task order award.

Item #	Description	GFI Estimated Delivery Date
1	BA ISEA IPT Plans, Processes and Procedures	30-days DATO

10.0 GOVERNMENT PROPERTY

As defined in FAR Part 45, Government property is property owned or leased by the Government which includes Government-furnished property (GFP) and Contractor-acquired property (CAP). Government property is material, equipment, special tooling, special test equipment, and real property.

GFP will not be provided and CAP is not anticipated on this task order.

NMCI computers will be utilized and assigned to contractor personnel. The contractor shall provide a list of all NMCI assets assigned to this order as part of the monthly TOSR (CDRL T001). Although NMCI assets are not reported as GFP, the contractor shall separately track and report all NMCI assets assigned to all contractor employees. At a minimum, the list shall provide asset description, name of contract personnel assigned the asset, the NMCI asset identification number, NMCI computer name, and the date the asset was assigned to the contract personnel. The contractor shall maintain the NMCI asset list throughout the life of the order. Prior removing a NMCI computer from a Government facility, the contractor employee shall possess at all times a Property Pass (OF-7) with the applicable NMCI asset identified. The contractor shall ensure all property passes are authorized and signed by the COR or other authorized Government personnel.

11.0 TRAVEL

11.1 LOCATIONS

Exact travel dates are not known at time of task order award, and locations are subject to change. The proposed travel locations identified are based on historical data. The contractor shall be able to travel to any of the sites listed below as well as sites noted in Potential Alternative Travel Locations.

Travel outside of the continental United States (OCONUS) which includes Alaska, Hawaii, and all foreign countries is required. The applicable countries are included in the list below as well as the potential list. Prior to travel, the contractor shall meet all necessary travel requirements for their company and personnel to support work in the noted foreign OCONUS sites.

Base Year and Option Years 1-4

# Trips	# People	# Days/Nights	From (Location)	To (Location)
1	1	10/9	Norfolk, VA	Austal, AL
2	1	10/9	Norfolk, VA	Mayport, FL
1	1	5/4	Norfolk, VA	Mayport, FL
2	1	10/9	Norfolk, VA	Pearl Harbor, HI
1	1	10/9	Norfolk, VA	Pascagoula, MS
3	1	10/9	Norfolk, VA	Everette, WA
1	1	10/9	Norfolk, VA	Marinette, WI
1	1	10/9	Norfolk, VA	Guam

1	1	10/9	Norfolk, VA	Gaeta, Italy
4	1	10/9	Norfolk, VA	Yokosuka, Japan
1	1	10/9	Norfolk, VA	Deveselu, Romania
1	1	10/9	Norfolk, VA	Rota, Spain
2	1	10/9	Norfolk, VA	Sasebo, Japan
1	1	10/9	Norfolk, VA	Redizikowo, Poland
2	1	5/4	Norfolk, VA	Newport RI
2	1	5/4	Norfolk, VA	San Diego, CA
1	1	5/4	Norfolk, VA	Washington, DC
1	1	5/4	Norfolk, VA	Cambridge, MA

POTENTIAL ALTERNATIVE TRAVEL LOCATIONS:

In addition to the travel details reflected above, it is anticipated that additional travel will be required. Those exact travel dates are not known at time of task order award, and locations are subject to change. The proposed travel locations identified below are based on historical data. The contractor shall be able to travel to any of the sites listed below as well as sites reflected above.

From (Location)	**To (Location)**
Norfolk, VA	Agana, Guam
Norfolk, VA	Amarillo, TX
Norfolk, VA	Atsugi, Japan
Norfolk, VA	Bangor, WA
Norfolk, VA	Bath, ME
Norfolk, VA	Beaufort, SC
Norfolk, VA	Bremerton, WA
Norfolk, VA	Cape Canaveral, FL
Norfolk, VA	Charleston, SC

Norfolk, VA	China Lake, CA
Norfolk, VA	Corpus Christi, TX
Norfolk, VA	Dalgren, VA
Norfolk, VA	Dallas, TX
Norfolk, VA	Deveselu, Romania
Norfolk, VA	Emerald Isle, NC
Norfolk, VA	Everett, WA
Norfolk, VA	Fallon, NV
Norfolk, VA	Fort Dix, NJ
Norfolk, VA	Forth Worth, TX
Norfolk, VA	Futenma, Japan
Norfolk, VA	Gaeta, Italy
Norfolk, VA	Genoa, Italy
Norfolk, VA	Groton, CT
Norfolk, VA	Gulfport, MS
Norfolk, VA	Havelock, NC
Norfolk, VA	Honolulu, HI
Norfolk, VA	Iwakuni, Japan
Norfolk, VA	Jacksonville, FL
Norfolk, VA	Jacksonville, NC
Norfolk, VA	Kaneohe Bay, HI
Norfolk, VA	Key West, FL
Norfolk, VA	Kings Bay, GA

Norfolk, VA	Kingsville, TX
Norfolk, VA	Kittery, ME
Norfolk, VA	Kuwait
Norfolk, VA	Lakehurst, NJ
Norfolk, VA	Lemoore, CA
Norfolk, VA	Manama, Bahrain
Norfolk, VA	Mayport, FL
Norfolk, VA	Meridian, MS
Norfolk, VA	Minneapolis, MN
Norfolk, VA	Miramar, CA
Norfolk, VA	Misawa, Japan
Norfolk, VA	Naples, Italy
Norfolk, VA	New Orleans, LA
Norfolk, VA	Newburgh, NY
Norfolk, VA	Newport, RI
Norfolk, VA	Nowra, Austrailia
Norfolk, VA	Okinawa, Japan
Norfolk, VA	Oklahoma City, OK
Norfolk, VA	Panama City, FL
Norfolk, VA	Patuxent River, MD
Norfolk, VA	Pearl Harbor, HI
Norfolk, VA	Pensacola, FL

Norfolk, VA	Ponce, Puerto Rico
Norfolk, VA	Pohang, South Korea
Norfolk, VA	Point Mugu, CA
Norfolk, VA	Port Hueneme, CA
Norfolk, VA	Quantico, VA
Norfolk, VA	Redzekowo, Poland
Norfolk, VA	Rijeka, Croatia
Norfolk, VA	Rota, Spain
Norfolk, VA	San Antonio, TX
Norfolk, VA	San Diego, CA
Norfolk, VA	Santa Rita, Guam
Norfolk, VA	Sasebo, Japan
Norfolk, VA	Seattle, WA
Norfolk, VA	Sigonella, Italy
Norfolk, VA	St. Augustine, FL
Norfolk, VA	Stuttgart, Germany
Norfolk, VA	Tucson, AZ
Norfolk, VA	Vallejo, CA
Norfolk, VA	Washington DC
Norfolk, VA	Whidbey Island, WA
Norfolk, VA	Whiting Field, FL
Norfolk, VA	Yokosuka, Japan
Norfolk, VA	Yuma, AZ

11.2 MEDICAL SCREENING FOR FLEET SUPPORT

Pursuant to COMUSFLTFORCOM/COMPACFLTINST 6320.3A, all contractor personnel (including subcontractors) embarking as members of the crew or as guest onboard a U.S. Naval vessels shall have current medical and dental screening and timely paperwork submitted as specified in the instructions. Those personnel with a significant chronic disease or condition that requires frequent medical monitoring and/or treatment shall not be allowed to embark/board any U.S. Naval vessel.

11.3 OCONUS TRAVEL REQUIREMENTS

Pursuant to SPAWARSYSCENLANTINST 12910.1B, DoDD 4500.54E, and the latest DoD Foreign Clearance Guide requirements, the contractor shall travel to OCONUS sites to support deployed forces. The contractor shall be familiar with and able to obtain approvals in the Aircraft and Personnel Automated Clearance System (APACS) as well as submitting and requesting letter of authorization (LOA) in the web-based Synchronized Pre-deployment & Operational Tracker (SPOT).

11.3.1 General OCONUS Requirements

The contractor shall ensure compliance with applicable clauses and travel guide requirements (including completion of any mandatory training) prior to traveling to each of the specified travel locations. The contractor shall be responsible for knowing and understanding all travel requirements as identified by the applicable combatant command (CCMD) and country. The contractor shall be responsible for submitting applicable deployment forms and/or deployment packages (CDRL A036) to the COR or task order technical POC and NIWC Atlantic Deployment Manager no later than 30 days prior to travel. For all OCONUS travel, the contractor shall submit an official OCONUS Travel Form (NIWCLANT 12990/12) and shall ensure all OCONUS travel has an approved APACS request. The COR will provide a blank travel form after task order award.

11.3.2 OCONUS Immunization Requirements

Pursuant to DoDI 6205.4, SPAWARSYSCENLANTINST 12910.1B, and any additional DON specific requirements, contractor employees who deploy to OCONUS locations both shore and afloat shall require up to date immunizations. The contractor shall review and verify if their personnel meet any immunization requirements prior to assigning personnel to travel.

11.3.3 Emergency Medical Screening for OCONUS Travel

During emergency related situations including health (e.g., COVID-19 pandemic) and weather-related circumstances, contractor personnel shall perform official OCONUS travel in accordance with the latest directions outlined in the NIWC Atlantic COG, related DoD travel websites, and the Centers for Disease Control and Prevention (CDC) website. To the extent possible, contractor personnel shall follow the same travel regulations and restrictions as Government civilian personnel. When in doubt concerning applicability, the contractor shall verify requirements with COR and NIWC Atlantic OCONUS Travel Team. Depending on the latest travel regulations which may differ based on location, contractor personnel shall be prepared to meet additional requirements such as medical testing prior to travel. These requirements will be identified by the COR. Contractor personnel shall complete any required health screening/testing and complete screening questionnaire which shall all be submitted to the COR prior to travel.

11.3.4 Letter of Authorization

The contractor shall have a LOA signed by the designated Contracting Officer for any and all OCONUS Travel. An OCONUS Travel Form (NIWCLANT 12990/12) is required for all travel locations OCONUS to include Alaska, Guam, Hawaii, Kwajalein Atoll, Johnston Atoll, Midway Islands/Atoll, Puerto Rico, US Virgin Islands, Wake Island, etc. If the travel location is not in "the lower 48"/CONUS, then an OCONUS Travel Form is required prior to the LOA being Government Authorized by an employee of the NIWC Atlantic OCONUS Travel Team in order for the Contracting Officer to approve. The LOA identifies any additional authorizations, privileges, or Government support that contractor personnel are entitled to under contract and task order, if applicable. The contractor shall initiate a LOA for each prospective traveler. The contractor shall use SPOT or its successor, at https://spot.dmdc.mil/privacy.aspx, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government’s interest, the contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed and approved by the SPOT registered Contracting Officer of this task order. Contractor personnel traveling in support of NIWC Atlantic shall travel with a hardcopy approved LOA in their possession.

12.0 SAFETY ISSUES

12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting

applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the task orders. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system. If performing within Government facilities, contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the Contracting Officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the COR or on-site Government representative.

12.1.1 Navy Shipboard/Submarine Support

In addition to the accident reporting requirements above, the contractor shall develop safety documentation (CDRL T037) in accordance with NAVSEA Standard Item 009-074 (Occupational, Safety and Health Plan) and submit the documentation to the Government for review; see applicable DD Form 1423 for additional reporting details and distribution instructions.

12.2 SAFETY EQUIPMENT

The contractor shall provide their personnel with any safety equipment required to perform work under this task order and the equipment must be in satisfactory working order. Personal safety equipment includes items such as hard-hats, safety shoes, safety gloves, goggles, hearing protection, non-flammable clothing for hot work personnel, gas/oxygen detectors for confined spaces, face shields, and other types of safety equipment required to assure a safe work environment and compliance with applicable federal, state and local safety regulations.

12.3 SAFETY TRAINING

The contractor shall be responsible to train all personnel that require safety training. Specifically, where contractors are performing work at Navy shore installations, that requires entering manholes or underground services utility the contractor shall provide a qualified person as applicable in 29 CFR 1910 or 29 CFR 1926 or as recommended by the National Institute for Occupational Safety and Health (NIOSH) Criteria Document for Confined Spaces. Also, when contractors are required to scale a tower, all applicable personnel shall have Secondary Fall Protection and Prevention training.

13.0 SUBCONTRACTING REQUIREMENTS

If the prime contractor is planning to utilize subcontractor(s) on this task order, the prime contractor shall identify the applicable subcontractor(s) in its proposal for the task order. Should the prime contractor be awarded a task order, only those subcontractors included in the proposal upon which the award is based are approved for use on the task order. Post award subcontractor additions (i.e. subcontractor additions to a task order after issuance of the order) are governed by FAR 52.244-2.

In addition, while Government consent to subcontract is not required for prime contractors with an approved purchasing system, if after award of a task order the prime contractor intends to enter into a subcontract with an entity not identified in its proposal upon which the task order award was based, the prime contractor shall nevertheless notify the Contracting Officer reasonably in advance of entering into any (i) cost-plus-fixed-fee subcontract, or (ii) fixed-price subcontract that exceeds either the simplified acquisition threshold or 5 percent of the total estimated cost of the task order. Such notification shall include, (i) a description of the supplies or services to be subcontracted, (ii) identification of the subcontract type to be used, (iii) identification of the proposed subcontractor, and (iv) the proposed subcontract price.

13.1 AUTHORIZED SUBCONTRACTORS

The following subcontractor(s) is either identified by the contractor at the time of award of the task order, have been consented to by the Government pursuant to the Subcontracts clause of the contract, or, in the event the contractor has an approved purchasing system, the contractor has provided notification in accordance with paragraph 13.0 above:

14.0 ACCEPTANCE PLAN

Inspection and acceptance is performed by the COR on all services, data, and non-data deliverables in accordance with the QASP, Attachment 1.

15.0 OTHER CONDITIONS/REQUIREMENTS

15.1 CONTRACT ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

Due to the type of work performed, there are organizational conflict of interest clauses that are applicable to this task order. The contractor shall follow the restrictions as cited in the applicable OCI clause(s) in Section H.

15.2 WORKWEEK

All or a portion of the effort under this task order will be performed on a Government installation. The contractor shall provide support services corresponding to Government workweek and core hours. Normal workweek is Monday through Friday. Pursuant to Federal law (5 U.S.C. 6103), the Government observes the following public holidays per year. For planning purposes, contractors working in Government spaces shall treat these holidays as Government non-work days which may affect accessibility to Government space.

Name of Holiday	Time of Observance
New Year’s Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth	19 June
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

If any of the above holidays occur on a Saturday or a Sunday, then such holiday will be observed by the Government on the prior Friday or following Monday, respectively.

15.2 EXTENDED WORK WEEK

Due to operational requirements, schedules, and the availability of required resources and/or downtime of those resources, extended work week (EWW) may be required for professional (i.e., salaried) employees.

15.3 NON-DISCLOSURE AGREEMENT (NDA) REQUIREMENTS

Contractors who receive or have access to proprietary information shall execute a Non-Disclosure Agreement (NDA) and submit to the COR prior to applicable work performance. Government and support contractors shall have access to the collaboration tool where appropriate non-disclosure agreements (NDAs) and Proprietary Data Protection Agreements (PDPAs) with the contractor are on file.

16.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

The contractor shall ensure all work accomplished utilizes the latest, relevant industry practices and standards when applicable unless otherwise indicated by text. In accordance with Defense Acquisition Policy, maximum utilization of non-Government standards will be made wherever practical.

16.1 REQUIRED DOCUMENTS

The contractor shall utilize the following mandatory documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the contractor shall meet requirements for any referenced document including subsequent updates applicable at time the task order request for proposal is posted.

	Document Number	**Title**
a.	DoDM 5200.01	DoD Manual – Information Security Program (vol 1, 2, 3) dtd 24 Feb 12 with Change 2/4/3 dtd 28 Jul 20
b.	DoDM 5200.02	DoD Manual – Procedures for the DoD Personnel Security Program dtd 3 Apr 17

	Document Number	Title
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12 with Change 2 dtd 20 Aug 20
d.	DoDM 5205.02	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08 with Change 1 dtd 26 Apr 18
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06 with Change 2 dtd 18 May 16
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program (NISP) dtd 18 Mar 11 with Change 2 dtd 24 Sep 20
g.	DoDI 5200.48	DoD Instruction – Controlled Unclassified Information (CUI) dtd 6 Mar 20
h.	DoDI 6205.4	DoD Instruction – Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense dtd 14 Apr 00
i.	DoDD 8140.01	DoD Directive – Cyberspace Workforce Management dtd 05 Oct 20
j.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14 with Change 1 dtd 07 Oct 19
k.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT) dtd 12 Mar 14 with Change 2 dtd 28 Jul 17
l.	DoD 8570.01-M	DoD Manual – Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12 and Change 4 dtd 10 Nov 15 (and subsequent replacement)
m.	DON CIO Memorandum	Acceptable Use of Department of the Navy Information Technology (IT) dtd 22 Feb 16
n.	SECNAV M-5239.2	Secretary of the Navy Manual – DON Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual dtd June 2016 (and subsequent revisions)
o.	SECNAVINST 5239.3C	Secretary of the Navy Instruction – DoN Cybersecurity Policy dtd 2 May 16
p.	SECNAVINST 5239.20A	Secretary of the Navy Instruction – DoN Cyberspace IT and Cybersecurity Workforce Management and Qualification dtd 10 Feb 16
q.	SECNAVINST 5510.30C	Secretary of the Navy Instruction – DoN Personnel Security Program (PSP) Instruction dtd 6 Oct 06

	Document Number	Title
r.	SECNAVINST 5510.36B	Secretary of the Navy Instruction – DoN Information Security Program dtd 12 Jul 19
s.	SPAWARINST 3432.1	Space and Naval Warfare Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
t.	SPAWAR AIPH	SPAWAR Afloat Installation Process Handbook (AIPH)
u.	SPAWAR SIPH	SPAWAR Shore Installation Process Handbook, Version 4 dtd 12 Nov 14
v.	SPAWARSYSCENLANTINST 3070.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Operations Security Policy dtd 20 Jan 17
w.	SPAWARSYSCENLANTINST 12910.1B	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Government and Contractor Personnel Outside the Continental Unlisted States dtd 23 Aug 16
x.	COMUSFLTFORCOM/COMPACFLTINST 6320.3A	Commander US Fleet Forces Command/Commander US Pacific Fleet Instruction, Medical Screening For US Govt Civilian Employees, Contractor Personnel, and Guests prior to embarking Fleet Units dtd 7 May 13
y.	Navy Telecommunications Directive (NTD 10-11)	System Authorization Access Request (SAAR) - Navy
z.	JTR	The Joint Travel Regulations (JTR) – Uniformed Service Members and DoD Civilian Employees
aa.	NIST SP 800-171	National Institute of Standards and Technologies (NIST) Special Publication (SP)
ab.	Section 508 of the Rehabilitation Act of 1973	United States federal law, as amended, 29 U.S.C. § 794d
ac.	Privacy Act of 1974	United States federal law, Pub.L. 93–579, 88 Stat. 1896, dtd December 31, 1974, 5 U.S.C. § 552a
ad.	NAVSEA SL720-AA-MAN-030	Navy Modernization Process Management and Operations Manual (NMP-MOM)

16.2 GUIDANCE DOCUMENTS

The contractor shall utilize the following guidance documents in support of this task order. The documents referenced in this section list the minimum version dates; however, the document's effective date of issue is the task order's request for proposal issue date.

	Document Number	Title

a.	SPAWARINST 3084.1	System Operational Verification Test (SOVT) Preparation and Execution Guide
b.	MIL-STD 196E	Joint Electronics Type Designation System
c.	SPAWARINST 4130.5	NAVWAR Handbook
d.	NAVSEA SL720-AA-MAN-010	NAVSEA Fleet Modernization Program Operations and Management Manual
e.	SPAWARINST 4130.3	NAVWAR Life Cycle Management Policy
f.	IEEE 12207.2.1997	Institution of Electrical and Electronics Engineers, Annex J (Informative)
g.	DoDM 1000.13-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, Volume 1, dtd 23 Jan 14
h.	DoDD 5000.01	DoD Directive – The Defense Acquisition System dtd 20 Nov 07
i.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System dtd 7 Jan 15
j.	ISO/IEC/IEEE 12207:2017	International Organization for Standardization/ International Electrotechnical Commission/Institute of Electrical and Electronics Engineers: Systems and Software Engineering – Software Life Cycle Processes
k.	ISO/IEC/IEEE 15288:2015	International Organization for Standardization/ International Electrotechnical Commission/Institute of Electrical and Electronics Engineers: Systems and Software Engineering – System Life Cycle Processes
l.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors dtd 27 Aug 04
m.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
n.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
o.	N/A	NIWC Atlantic Public website – CICO Procedures https://www.public.navy.mil/navwar/atlantic/pages/contractorcheckin.aspx
p.	N/A	NIWC Atlantic COG page – Procurement Role ERP https://wiki.spawar navy mil/confluence/x/uQGRBg
q.	N/A	NAVWARSYSCOM Code 80330 mandatory training webpage – https://wiki.spawar navy mil/confluence/x/jwDsAQ
r.	N/A	DoD Foreign Clearance Guide – https://www.fcg.pentagon.mil/fcg.cfm

16.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents necessary for performance on this task order. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization’s website.

[END OF PWS.]